Inadvertent Covert Channels

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

The editing marathon continues. A chapter on instant messaging and collaboration tools prompted the following thoughts.

One morning a few weeks ago, I looked at my Skype icon and found that there had been a Skype call the night before. I found two 10-minute messages left on "voice-mail" through Skype several hours after I shut down my computer. The first couple of minutes was a perfectly normal recorded message from a colleague – but the remaining 18 minutes were sounds from his office! He had forgotten to terminate the call, so Skype obediently recorded everything the microphone could hear. I don't know if he noticed at all, because the second call was exactly 10:00 minutes long – an unlikely length had he terminated the session deliberately. I still have no idea what happened to prevent a third segment from being recorded.

This incident was unusual only in that it was a voice-mail recording. There are many times I have been in a Skype conversation, either with or without video, and have had to terminate the call myself because the person who initiated it forgot to click the red "end call" symbol. Failing to do so creates an unintentional covert channel for data transfer – which usually doesn't matter in casual conversations but which could be a serious problem in a business context.

A covert channel is a data transfer medium that is not known to the data owner. For example, a wiretap on a phone line or a man-in-the-middle attack on a wireless data connection are covert channels. Steganography, in which some tools insert the desired message into the low-order bits for pixel colours, is an example of using a covert channel for data transfer.

Another danger with instant-messaging clients is that the focus of one's typing can shift from a password-entry field into an instant-messaging field without one's notice; I have personally felt like (OK, been) a complete fool for typing password into a Skype message – and sending it (thankfully) to my wife, who very kindly purged the Skype history for our conversations. Imagine if I had done that to the Skype message field for anyone else! I can see it now: someone posts a screenshot of my password in their Skype client – if I thought that libelling a computer manufacturer by mistake a few years ago was bad, such an error would surely have increased the number of hits for "Kabay idiot" in Google to astronomical levels.

A common covert channel when people use faxes (and apparently, there were 16B faxes sent last year!)< http://www.slideshare.net/RingCentral/facts-about-global-fax-usage > is to send the fax to the wrong fax number. In 2006, a report surfaced that "A small Lockport, Manitoba-based distributor of herbal remedies has for the past 15 months been mistakenly receiving faxes containing confidential information belonging to hundreds of patients with Prudential Financial Inc.'s insurance group. The data exposed in the breach -- and faxed to the company by doctors and clinics across the U.S. -- included the patients' Social Security numbers, bank details and health care information."< http://www.computerworld.com/s/article/108429/Confidential_patient_data_sent_to_wrong_company_for_15_months?taxonomyId=017 > The doctors and clinics were using the wrong number

for their faxes – only one digit different from that of the insurance company – and swamping the tiny North Regents company with thousands of unwanted, highly confidential faxes. Prudential insisted that its fax number was correctly indicated on all its documents and correspondence, and said that it could not be held responsible for misdialling by its customers. Indeed, the large company told the small company that "Effective immediately, North Regent RX will forward to Prudential Financial all faxes it has received, as well as any it may receive in the future." This solution was wholly impractical for the tiny group, who offered to change their toll-free number if Prudential would pay for the costs of reprinting all its advertising, business cards and letterhead. Prudential declined to do so.

Some people (I am, with effort, refraining from characterizing their degree of intelligence) use old email messages as a basis for sending out new ones using the REPLY ALL function – and without verifying whether the distribution list is appropriate. Simply choosing the wrong list can also lead to trouble, as Sherri Goforth discovered when that Tennessee Republican bigot (no hesitation here) sent a racist image sneering at President Obama to "the wrong list" – and had it posted on the Web.< http://www.cnn.com/2009/POLITICS/06/16/tennessee.email/ >

Another inadvertent covert channel is simply hitting REPLY ALL by mistake – and sending inappropriate messages to people who shouldn't receive them. In 2010, an advertising director wrote a message using inappropriate ("locker-room" was his term) language to criticize colleagues to a teammate in an internal competition – and used REPLY ALL by mistake, sending the email to 200 people – including the people he was criticizing.< http://online.wsj.com/article/SB10001424052748703386704576186520353326558.html > And then there's the problem of a REPLY ALL message asking "Take me off this list" or "You used REPLY ALL, you fool" and generating waves of angry third- and fourth-level REPLY ALLs. In January 2009, someone in the US State Department sent a blank message with several thousand recipients visible in the TO or CC field; replies using REPLY ALL caused a denial of service by swamping the internal email servers.< http://www.huffingtonpost.com/2009/01/10/replyall-email-storm-hits_n_156856.html >

Basic good sense to avoid inadvertent covert channels in email include using the BCC field for the distribution list to prevent foolish distribution of replies.

For more guidance in effective use of email, see "Using E-mail Safely and Well"< http://www.mekabay.com/infosecmgmt/emailsec.pdf >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *