Prescription for Failure

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

One of the concepts I've always enjoyed pointing out to my young students is the *side channel.* We were just discussing monitoring and control systems in the IS342 Management of Information Assurance< http://www.mekabay.com/courses/academic/norwich/is342/index.htm > course (PPTX slides< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch53_monitoring_control.pptx > and PDF notes< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch53_monitoring_control.pdf > freely available) and one of the issues that came up was how to indicate a problem in a monitored system. "If we're monitoring the network and it goes down, how do we tell anyone it's down?" The students rightly piped up, "Use another communication medium" and we discussed walking over to tell someone, posting a paper note as a warning, generating robotic voice status updates via phone, sending text messages using SMS (Short Message Service) to mobile phones, putting information on electronic dashboards for situational awareness using separate networks, and other side channels.

Another case where side channels play an important role in *breaking* security is data-loss prevention (DLP)< http://csrc.nist.gov/groups/SNS/rbac/documents/data-loss.pdf >. A primitive DLP is the Acrobat security feature that can lock a file against copying or printing by using a password to allow such functions. Unfortunately, the password security is weak; entering "crack acrobat password" into a search engine brings up thousands of hits for free or commercial password-cracking software tailored to attack secured PDF files.

Some DLP systems use kernel-level modifications to prevent such functions as copying, modifying, printing, email, screen captures and so on. For example, McAfee Data Loss Prevention software< http://www.symantec.com/data-loss-prevention > provides control over

- Input/output (I/O) involving removable media such as flash drives;
- Restricting what can be attached to email messages;
- Blocking printing on all but specified printers;
- Controlling uploads to Websites;
- Blocking the use of screen captures.

Unfortunately, none of these products can stop a disgruntled employee turned industrial spy from snapping a photo of a screen or printed page full of valuable, confidential information using her mobile device camera. Even ordinary cell phones now have unprecedented pixel densities; for example, the Samsung Galaxy Note II has a back-facing camera that provides 8 megapixels. I didn't even bother looking further for the even higher density devices I'm sure exist already or are coming soon.

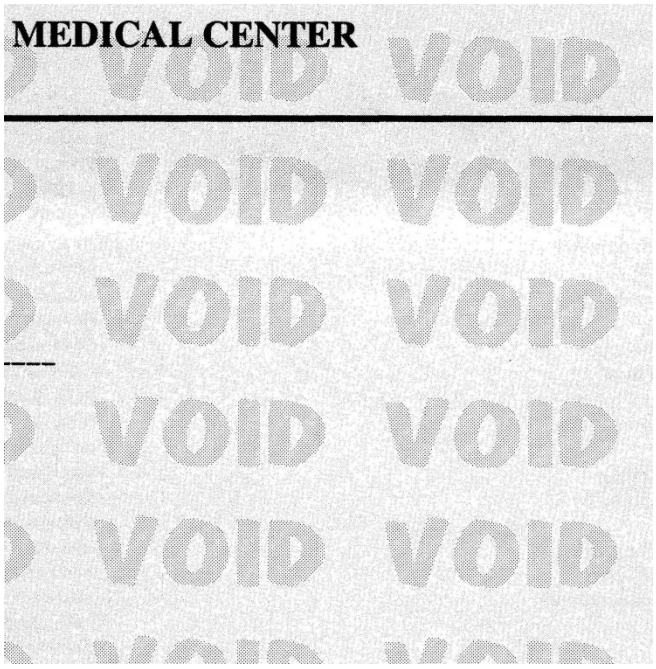
Beyond photographs or movies, cell phones and tablets have microphones: it is trivial to initiate a recording and then slip the screen-darkened phone into one's carrying case or jacket pocket.

There's a reason that organizations using sensitive compartmented information facilities (SCIFs – see for example SCIFSOLUTIONS< http://scifsolutions.com/ >) complement their Faraday cages with strict rules on exactly what electronic equipment is permitted past the security guards at the entrance to the secured portions of the building. The whole point of a SCIF is to prevent unauthorized data leakage using side channels; allowing someone secretly to record a top-secret conversation with a cell phone would be silly.

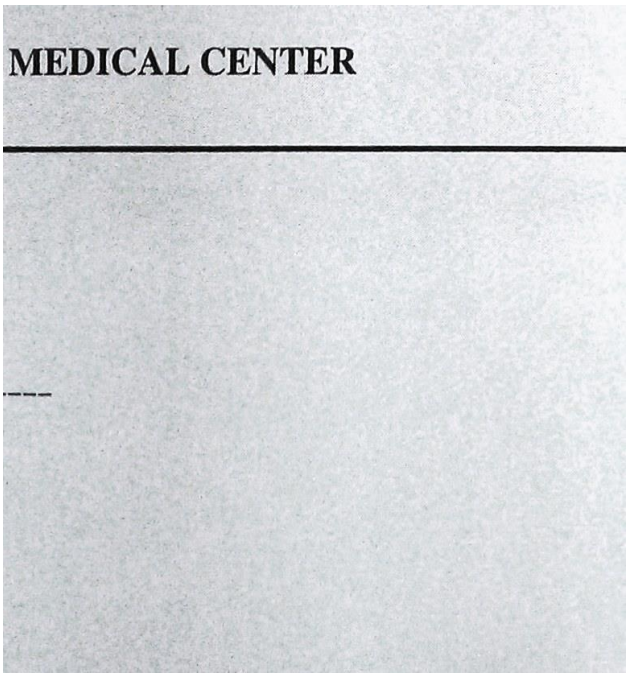
A classic use of side channels is steganography< http://www.garykessler.net/library/steganography.html >, which refers to hidden writing – information transfer in non-obvious forms such as integrated into music, photographs, videos, Web pages and so on. Unlike cryptography, which alters cleartext into ciphertext that is usually immediately obvious, steganography conceals even the existence of the message. A microdot could be considered a steganographic technique, since unless one knows which dot on a printed page is actually a microphotograph readable through a microscope, one is unlikely to know that there's a secret message at all.

Recently I discovered a failed form of DLP when I was given a prescription during an unfortunate visit to an emergency room (I have ripped my right leg's hamstring muscle with agonizing consequences). I scanned the prescription so I could send it to my wife (since I can't drive now) by email (because I forgot to give it to her when she left in the morning) to pick up a pain-killer that won't make me crazy (I become agitated and violent when given ordinary narcotics)(really). Here's a section of the resulting scan< prescription_scanned_close-up.jpg >:

This is great, right? The actinic light of the scanner brought out a completely invisible marking to warn pharmacists that someone is presenting them with a copy of a prescription – a copy possibly modified for evil purposes.



Unfortunately, the method is limited. Here's the same area of the paper photographed in ordinary fluorescent light on my desk using my cell phone camera< prescription_photographed_close-up.jpg >:



Oops. No VOID marks.

I'm reporting the problem to the head of the pharmacy at the hospital, with a request that the alert be passed up the chain to the people who (a) created the paper and (b) ordered it to be used for prescriptions.

There are many methods for making paper difficult to duplicate; experts who manage the money supply< http://www.moneyfactory.gov/anticounterfeiting.html > have invented high-resolution printing with subtle colours, insertion of plastic bands with authenticating information, and so on. All of these cost extra, but at the very least, the people who created the non-copy paper should have checked the possibility of a simple photograph in ordinary light before releasing their special product.

Failing to think outside our preconceptions is a prescription for failure.

* * *

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/ >

* * *