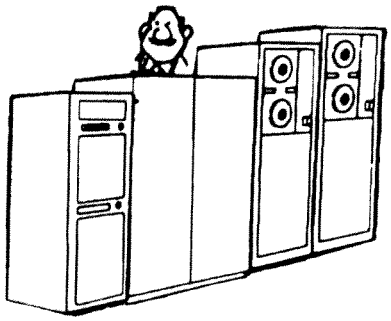

Some Reflections on the Reality of Computer Security (U)

by Robert J. Hanyok, H215

(U) Along with the tremendous growth of our computer usage in recent years, we have become aware that we need security measures that will protect the computer, databases, and associated programming. We have developed a host of techniques and plans in response to this need, including access restrictions, passwords, audit trails, encryption, etc. Security officers have been generally enthusiastic in carrying out these measures. As a result, the users have insisted that the resulting security of their systems is ironclad and invulnerable. On paper their claims seem valid, but beneath those claims is a reality that belies this so-called "security."

(U) Here I should establish two points. First, this paper is a personal impression of computer security practices. It is not an analysis of particular security modules, equipments, or kernels; nor is it intended to be exhaustive in scope. The aim is to illustrate the so-called human factor shortcomings I have encountered, examples of which all occurred on computer systems having one or more security measures.

~~(C)~~ Second, my observations are based on more than two years' work in the S organization, where I was involved in evaluating the security frameworks of various computer systems used by NSA, DoD, other federal agencies, and by contractors. I helped develop the Computer Security Survey System (CS^3) which became a major tool in analyzing the security elements of these systems. CS^3 provided a prioritized, coherent, and quantitative method of evaluating computer system security. The use of CS^3 provided, for me, the first inklings of the reality of computer security practices.

(U) Just what is the reality of computer security? The reality is that computer security measures are often undercut by user practices and less-than-adequate implementation. There are three elements to this reality that I have observed. To a degree they are interactive. They all have one trait in common: they are not obvious in a system level review.

~~(C)~~ User level security practices vs. system level security measures.
The user does not fully use the security measures that are available on the computer system. Some techniques, like audit trails, are now controlled by the system and operated with the user ordinarily unable to intervene, alter, or negate them. But some measures, by their nature, allow the user much latitude. The most common case I encountered was with passwords. Some systems levied length requirements for passwords; some did not. Source and randomness of passwords were ill-defined. The result, of course, was that while everyone had passwords, they could be too few characters, predictable, and often kept in accessible places. In one office we visited, the operators had taped their passwords to the terminals. In another system, unauthorized persons were given passwords for "special projects." At best, such practices can be labelled sloppy; at worst, they are an outright invitation to compromise.

~~(C)~~ User security practices are dictated, not by the classification level of the data, but by the perception of the threat.
This was probably the most unexpected phenomenon I encountered--almost a reversal of conventional security imperatives. While some users who handled sensitive data in their

~~(FOUO)~~ This is the time of the year for coming and going, so a word about the distribution of CRYPTOLOG might be useful.

~~(FOUO)~~ Our distribution is to organization and to individuals within the NSA headquarters, and to organization only outside the immediate area of the headquarters. Because of the technical nature of the various articles and items in CRYPTOLOG, it should not go outside the technical community. Even articles that are marked as UNCLASSIFIED should not be taken outside the work area, unless cleared by [redacted] Q44, x3085s or 688-6524 (see CRYPTOLOG, May 1982, page 4, fourth paragraph).

~~(FOUO)~~ When subscribers move to a job outside the headquarters area, we can send the magazine to the organization, but not to the individual. When you return, a phone call or note to [redacted] P14, Room 8A177, x3369s, will get you back on the distribution list by name.

(U) Until now, the month that each CRYPTOLOG issue carries on the cover has been the month we go to press, but this has been confusing to some, because the readers didn't see the issue until the following month. Thus, the April issue didn't appear on your desk (or wherever you get your mail) until May. So, this issue becomes the June-July issue, and future issues will carry the name of the month in which (we hope) they appear.

(U) We have been sending each issue to the printer somewhere around the middle of the month, and the process of printing and distributing has been taking about a month. This means that our deadline for material is roughly the 10th of the month, give or take a day for intervening weekends. If you want to get something into a specific issue, give us a call and let us know how much space to hold for you.

Solution to NSA-Crostic No. 40

"Rules for the Camel Corps,"
[redacted] CRYPTOLOG,
March 1982

"It is frightening to contemplate the amount of time [we] NSA employees spend in meetings. There are staff meetings at all [echelons], meetings to solve a particular problem, club meetings, and even meetings to find reasons for more meetings. 'He's at a meeting' is all too frequently heard on the other end of a phone call."

P.L. 86-36

From: phr at CARONA
Subject: Editorial comment
To: cryptolg at barlc05
cc: phr

Hi,

(U) Just received my May 1982 issue of Cryptolog and read with suprise the editorial on moving. I would like to share with you my theory on the need to keep moving within the Agency. Clearly, there is at least one too many organizations in the Agency. Therefore, it is imperative to keep one organization in a moving van or stacked in the halls at all times. I am astonished that in all your years at NSA, you have not reached this same logical explanation. NSA is a giant version of one of those puzzles that have 35 numbered sliding pieces with one blank hole. SOMEONE is trying to get all the offices into numeric order but the speed with which we reorganize around here constantly frustrates THEIR efforts and causes the constant moving we MUST ENDURE.

Thank you,
[redacted]
T441, 1181s
phr@carona

P.L. 86-36