HOW TO TELL AN HONEST PROGRAMMER

John M. Carroll
Computer Science Department
University of Western Ontario
London, Ontario

ABSTRACT

ABSTRACT

The weakest aspect of any posture taken to perserve the privacy or confidentiality of data resident within computers in the inordinate amount of trust that must be placed in programming personnel. This situation suggests that steps should be taken to define criteria for selecting job condidates who are honest and reliable. This paper described an approach to this problem and presents a few tentative results.

RESUME

La principale faiblesse de n'importe quelle mesure prise pour préserver le secret ou la confidentialité des données entrées en ordinateur réside dans la confiance inhabituelle qu'on doit accorder au personnel de programmation. Cette situation invite à prendre des dispositions pour définir des critères nécessaires au choix de candidats honnêtes et fiables. Cette étude décrit une solution possible à ce problème et présente quelques résultats expérimentaux.

FOOTNOTE

The support of the National Research Council, grant number A-7132, and of the Canadian Certified General Accountants' Association are gratefully acknowledged.

INTRODUCTION

Certain vulnerabilities inherent in remotely accessed resource-sharing computer systems arise from the fact that management must repose a great deal of trust in its senior systems programmers. Indeed, the information security manual used by the British government states that

> Unless and until it shall have been proved to the contrary, it shall be assumed that no security features can be relied on, either individually or in combination, to protect information from an unauthorized person who has good knowledge of the system and who has, can acquire or can simulate the authority to enter the computer room, submit a job over the counter, or operate a terminal.

OBJECTIVES

Historically, there have been only two means to ensure that loyal and reliable individuals are hired or promoted into positions of trust. The first is a thorough investigation of each candidate's background; the second is examination of the candidate by use of the polygraph. Both of these methods have their limitations and both raise grave civil rights issues.

The objective of the work to be described is to develop methods by which to detect potential computer abusers within the constraint that such methods not contravene the candidate's civil rights.

It was decided to explore the possibilities of using a paper-and-pencil test supplemented by analysis of the candidate's discourse and handwriting.

TEST MATERIALS

The test consisted of eight parts. All questions were in true-false format.

Part one was a difficult test of skill replete with opportunities for cheating and as such provided a measure of the candidate's honesty [2].

Part two was a test for accident proneness [3].

Part three was the Luescher colour preference test, sometimes used in personnel screening [4].

Part four consisted of twenty questions intended to measure the candidate's job dissatisfaction [7].

Part five consisted of twenty-five questions that elicited expression of the candidate's social attitudes [1].

Part six consisted of twenty-six questions that asked for the candidate's judgement as to whether a particular action was ethical or not [6].

Part seven was answered by a short essay and was contrived to obtain material for handwriting and discourse analysis.

Part eight asked whether the candidate had participated in twelve specific incidents of computer abuse. Table I is a list of these acts keyed to the numerical designation to be used in subsequent sets of data.

The handwriting analysis consisted of measuring forty characteristics of the examplar taken in part seven [5].

Discourse analysis had not been completed by the deadline for papers for this conference.

METHOD OF TESTING

The test was administered anonymously to fifty-nine third-year general and seven fourth-year honours computer science students at the University of Western Ontario in September 1977.

Scoring of the independent variables was done on a three-point scale. Plus one always represented the most unfavourable answer, such as confession to an act of computer abuse, assertion that an act contravening a code of ethics was indeed ethical, affirmation of an anti-social attitude, agreement with a factor of job dissatisfaction, display of a characteristic usually considered "negative" by graphologists, a score so high on the test of skill as to have required cheating, a test score indicating accident proneness, or a "negative" choice of colours (eg. a dislike of the colours red, blue, green, and yellow and a fondness for gray, black, brown and purple.)

Minus one represented the diametrically opposite answer or characteristic; zero was reserved for no answer or for a neutral characteristic.

The dependent function was whether or not the subject was a computer abuser; it was decided on the basis of whether he/she confessed to half or more of the enumerated acts.

ANALYSIS

The test scores were first analyzed by stepwise multiple linear regression. See Table II for a summary of the results of this exercise. Table III is a summary of the parts of the test with the numerical designations that key then to the regression table.

Next a 130-by-130 intercorrelation matrix was computed. This matrix arrayed the data necessary to assign to each test item a score on an open-ended geometric scale. Each characteristic or answer showing an inter-correlation of 0.40 or higher with any act of computer abuse, was awarded eight points. Those showing an inter-correlation of 0.30 to 0.40 were awarded four points; those showing an inter-correction of 0.20 to 0.30 were awarded two points. Twenty-one answers or characteristics attained scores of ten or more. See Table IV for a listing of these test items, arranged in descending order of their scores.

Figure 1 illustrated graphically the fact that three or more inter-correlations of 0.20 or more were found to bind together the acts of computer abuse numbered 1, 2, 5, 10, and 11. Actions 4 and 9 are bound by only two such inter-correlations. On the other hand, acts 3, 6, 12, and 7 are bound into a separate nexus entirely. Action 8 stands by itself.

OBSERVATIONS

Superficially one might be led to conclude from context that actions 1, 2, 5, 10 and 11 (and to a lesser extent: 4 and 9) are specific to the computer environment and therefore characteristic of the so-called "systems hacker" who is probably the real nemesis of computer security.

Actions 3, 6, 7, and 12, although occurring here in a computer-science environment, could, in fact, happen in virtually any classroom environment.

Action 8 is not necessarily an act of computer abuse at all; sometimes this act is sanctioned for educational purposes. It was a poor choice for a question. Nevertheless, its relative isolation should tend to enhance confidence in the experiment as a whole.

There is a relatively high positive slope coefficient associated with unethicality. The coefficient had extremely high statistical significance. One may, therefore, conclude that a lack of ethics is the most poignant characteristic of the computer abuser.

The fact that the lack of ethics is the single best predictor of potential computer abuse, is a persuasive argument for introducing courses designed to enhance professionalism in the educational fields that relate to informatics.

There was a low negative slope coefficiant associated with dissatisfaction that had high statistical significance. This fact suggests only that computer abusers are happy in their work.

All the other slope coefficients had standard errors greater than their mean values, which makes one reluctant to place much credence in them. Three did show statistical significance, however.

In the case of accident proneness, there was a slight negative slope suggesting that, if anything, the computer abuser possesses somewhat greater dexterity than other informaticians; quite possibly he/she needs it.

Antisociality showed a small positive slope, as did handwriting.

There was no statistical significance in either the colour preference test or the measure of dishonesty.

Examination of the list of test items selected from the 130-by-130 inter-correlation matrix revealed that it included sixteen questions that computer abusers answered in ways contrary to codes of professional ethics. There were also three social attitudes that were significant; the one (V-4) could be interpreted as the "lawless frontier" syndrome - or, in other words, "If there are no generally accepted rules, how can they be broken?" A second attribute (V-7) recalls the familiar differential association syndrome - which may be articulated as: "Everybody else's doing it, so why not me?". A third attribute (V-25) appears to be congruent with the ever-popular justification of the young for any of their irresponsible actions; that is, "If an act doesn't hurt some particular individual, it isn't wrong".

Only two test items from the handwriting area displayed high scores based on inter-correlations. One was a positive correlation with rightword sloping letters (VII-21), but this characteristic is typical of ninety percent of the population. The other characteristic observed (VII-3) was a lack of firm pressure on the finish strokes of words. This is by no means a universal characteristic and may be potentially useful in personnel screening.

CONCLUSION

In summary then, your typical computer abuser; in addition to being young and handsome and bright, as are all my students; is a well-adjusted person; basically honest inasmuch as he or she probably wouldn't lie to you; and is a fast and accurate worker.

On the debit side, however, they have, like many persons in their age group, become aculturated to the "rip off" as a way of life.

Most importantly, the typical computer abuser hasn't got the vaguest idea of professional ethics. It has never occurred to him or her that computer time represents money and, more importantly, that the information stored in computers represents not only money, but personal reputations as well; and quite possibly, the security of the nation. On the other hand, we can go this far and no further in painting the computer abuser with a broad brush, because there are at least two sub-species of computer abuser: the systems hacker, and the garden-variety crook (defalcator/defalcatrix americanus/americana). Perhaps there is an even finer structure than that. For this reason broad generalities may not be very helpful in identifying potential computer abusers.

I am starting now to re-study these test data using the powerful techniques of the analysis of correspondence - widely used in Europe but new to many in North America. I am also going to look for significant correlations between abuse actions and the measurable characteristics of the computer abuser's discourse. Further down the road, when and if spoken input to computers becomes feasible, one might conduct a screening test as part of a preemployment interview. Such a test could then be correlated in real-time with data obtained from physiological measuring equipment using non-contacting sensors such as voice-stress analysers, wiggle seats, or infrared scanners.

Given such embellishments, it would quite likely be possible to make accurate inferences regarding an individual's potential for defalcation without having to rely on polygraphs, background investigation or voluminous files of personal information.

These computer-based techniques have the potential for allowing us to screen out persons with whom it would be risky to form relationships. They could very well make other more distasteful methods of screening obsolete.

. Such as discriminating against people on the basis of race, national origin, age, sex, or religion presumably so as to surround ourselves with people like ourselves whom we feel (often contrary to fact) that we can trust.

. Such as compiling extensive dossiers of personal information that we believe might someday be relevant to making a decision about someone. Meanwhile choking our computer resources with an overwhelming glut of irrelevant information about nobodies that will never be needed.

. Such as carrying out extensive physical or electronic surveillance of persons regarding whom we must imminently make a decision.

. Such as wiring a candidate into a lie detector to get results that for some purposes with some people can be 90 percent accurate and that for other purposes or with other people can be 90 percent wrong.

We can, instead, hopefully arrive at the point where we can draw accurate inferences from a small sample of the candidate's observable behaviour.

Wherein the potential loss-causing individual will give himself or herself away the minute he or she walks in our door or opens his or her mouth.

REFERENCES

(1) Ash, 1971, Screening Employment Applicants for Attitudes Toward Theft, Journal of Applied Psychology, Vol. 55, pp. 161-1964.

(2) Bernard and Leopold, 1962, "Test Yourself", Chilton Book Co., Rednor, PA.

(3) Block, 1975, A Test That Tells Who Is Accident Prone, Psychology Today.

(4) Curtis, (undated), "Curtis Color Test", Bob Curtis-Management Consultant, Dayton, OH.

(5) Holder, 1958, "You Can Analyze Handwriting", Prentice-Hall, NJ.

(6) Parker, 1976, "Crime By Computer", Charles Scribner & Sons, NY.

(7) Profit, 1975, Job Satisfaction Analysis, Engineering Digest.

TABLE I - CITED ACTS OF COMPUTER ABUSE

1. Attempting to find out how unpublished commands work so you can use them.
2. Trying to LOGON a system of which you are not an authorized user.
3. Exchanging programs with other users without authorization.
4. Trying to do things at terminals that are not described in user manuals.
5. Trying to penetrate the security of a system.
6. Using a program written by another person as if it were your own.
7. Submitting a program developed in one course as part of the project work in another.
8. Using computer time for personal recreation.
9. Trying intentionally to "crash" a system.
10. Trying to obtain computer time without being charged for it.
11. Improperly using another person's password.
12. Using a TALK circuit to harass operators and other users.

TABLE II - ANALYSIS OF TEST RESULTS

Part of Test	Slope Coefficient B	Standard Error of B	Level of Significance %
VI	.244	.044	0.1
V	.061	.075	4
I	.015	.020	7
II	-.043	.045	3
III	-.152	.279	6
IV	-.126	.085	1
VII	.038	.054	5
(constant)	1.606	1.170	

TABLE III - PARTS OF QUESTIONNAIRE

I Dishonesty (test of skill with opportunity to cheat)
II Accident-Proneness
III Luescher Colour Preference Test
IV Job Dissatisfaction
V Agreement with Antisocial Statements
VI Assertion that Acts Contravening Codes of Ethics are Ethical
VII Handwriting Characteristics

TABLE IV - MOST HIGHLY CORRELATED TEST ITEMS

Item		Correlation Score
VI-12	It is ethical to accept the challenge offered by a time-sharing service to penetrate its security.	22
VI-8	It is ethical to offer the use of a program written at your employer's expense to a friend without your employer's permission.	20
VI-6	It is ethical to use a password you discovered accidentally.	18
VI-11	It is ethical to attempt to do through a terminal things not described in user manuals.	18
VI-2	It is ethical to use a program despite comment statements telling you not to.	18
VI-16	It is ethical to use proprietary programs in ways that avoid paying for their use.	16
VI-21	It is ethical to do homework for one course on an account set up for another course.	16
VI-24	It is ethical to use a school account to set up an inventory system for a downtown merchant.	14
VI-25	It is ethical to read proprietary documentation without authorization.	14
VI-26	It is ethical to rummage through trash for interesting program listings.	12

(continued)

Item		Correlation Score
VI-15	It is ethical to develop your own programs using your employer's facilities.	12
V-25	I believe that unlawful acts are wrong only when they hurt another individual.	12
V-4	I believe that there is no such thing as programming malpractice because standards do not exist.	12
VII-3	Pressure light on finish strokes of words.	12
VI-3	It is ethical to try to discover unpublished commands by trial and error.	10
VI-4	It is ethical to attempt to learn another user's password.	10
VI-13	It is ethical to carry on personal conversations over a computer communications system.	10
VI-14	If granted access to a police system to check out a program, it would be ethical to look up the record of a friend.	10
VI-23	It is ethical to copy systems load modules onto tape and take them with you when you change jobs.	10
V-7	I believe businessmen often intentionally bill customers twice in hope they will pay both bills.	10
VII-21	Small letters slope to the right.	10

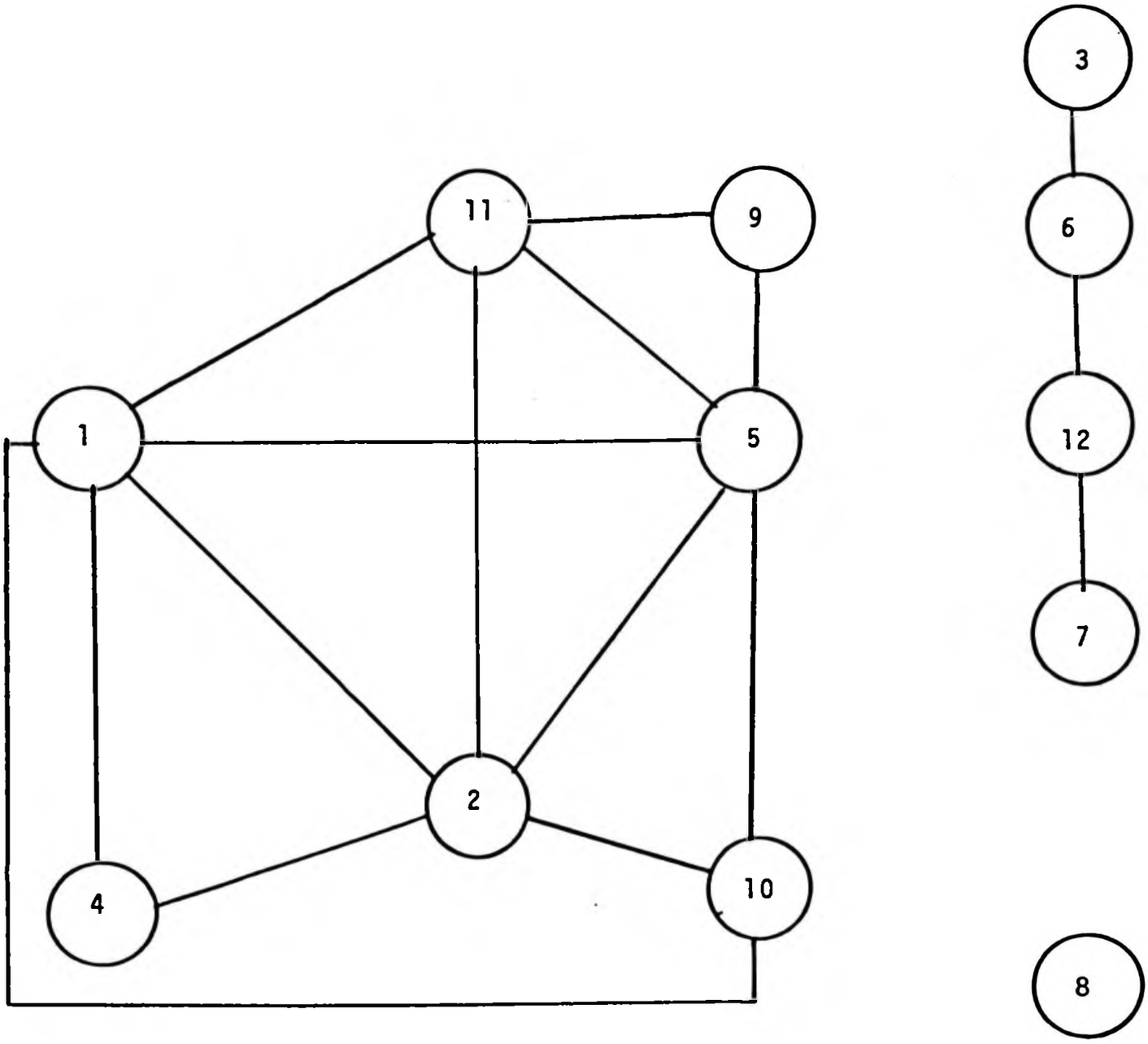

Figure 1. Clustering of incidents of computer abuse.