Beyond Technical Security:
Three Principles for Life

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

On Wednesday the 24th of April 2013, the School of Business and Management< http://programs.norwich.edu/business/ > at Norwich University celebrated the induction of a dozen students into the computing honour society Upsilon Pi Epsilon < http://upe.acm.org/ > and of the business and management students into Delta Mu Delta < http://deltamudelta.org/ >.

We had a splendid supper and pleasant conversation, and then our Director Dr Najiba Benabess < http://www.linkedin.com/pub/najiba-benabess/38/277/531 > led us through the evening's celebrations.

When everything was finished, Dr Benabess and I played a trick on our captive audience. She introduced me as the last speaker of the evening, and by arrangement, turned to me and said severely, "Now remember, Prof Kabay, no more than 40 minutes!" I looked pained and complained that I didn't see how I could fit all my advice into only 40 minutes. I told the students and faculty that I'd try to fit everything in, but that I had a great deal to give them and they should loosen their belts and get relaxed, because this would take considerable time.

By this point, most of the people in the audience were looking at their watches and looking downcast at the prospect of yet another speaker – especially one complaining of having only 40 minutes.

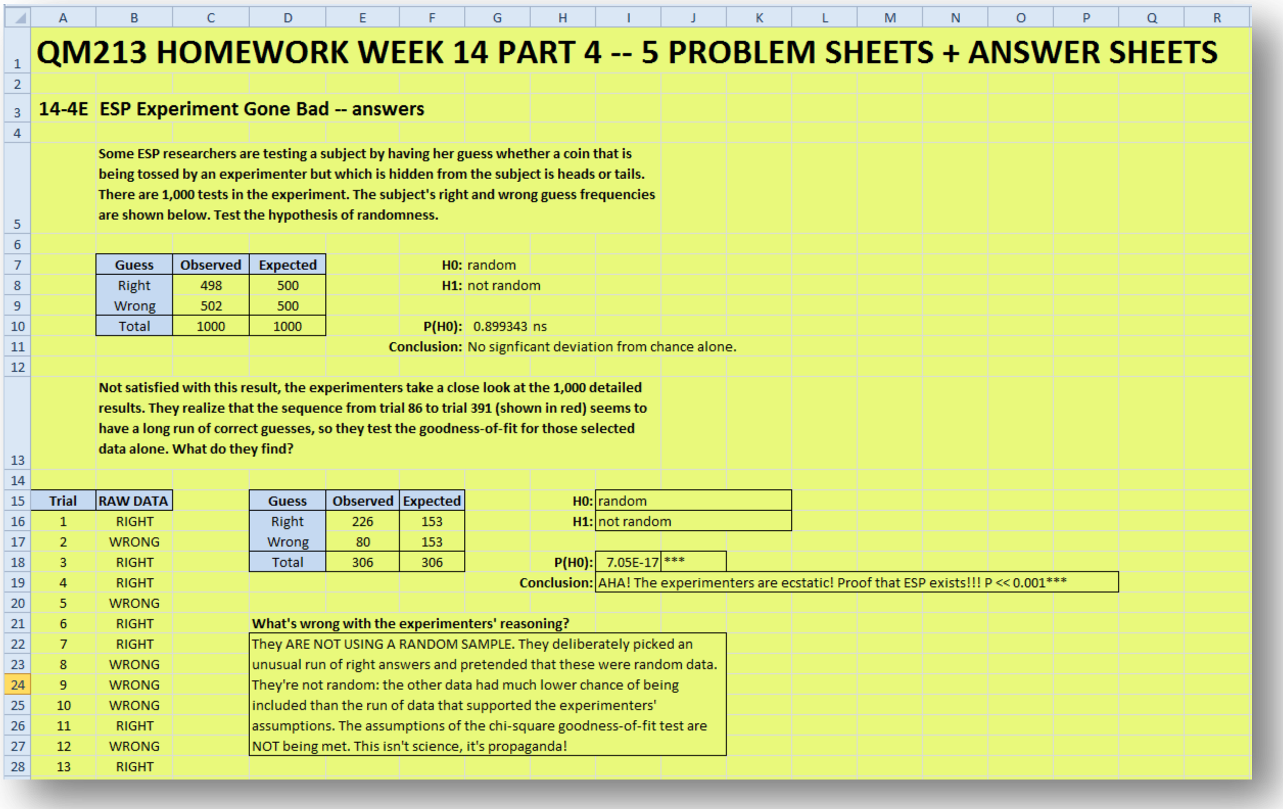
My actual speech took about 90 seconds and made three points. I've expanded my comments to take advantage of this written format.

1. **Question Authority.** Don't ever let social or professional status get in your way of thinking critically and sceptically. If something you're being told or told to do doesn't make sense, ask questions (politely) until it does – or until you and your interlocutor understand that the initial instructions or statements were wrong or need clarification. If you don't understand what an expert is saying, say so: ask for clarification. You don't have to interrupt a public lecture – be sensitive to context – but you shouldn't let the issue slide.

   My favourite story about questioning authority is from the 1980s when I taught at John Abbott College< http://www.johnabbott.qc.ca/welcome > in the west end of Montreal Island< http://ville.montreal.qc.ca/portal/page?_pageid=5977,86481579&_dad=portal&_schema=PORTAL >. I took my database students (from the John Abbott Programmers Course, JPC) to Place Ville Marie< http://www.placevillemarie.com/en/home.php > for a lecture by a major vendor about their newest database software. There were about 300 professionals in the audience. Partway through the lecture, the speaker said something like, "And we used the matrix-analytical method to optimize the design." I put up my hand. "Yes?" said the speaker. "I'm sorry," I said apologetically, "but I don't know what the matrix-analytical method is." The speaker stared at me in horror for a moment. He burst out, "Neither do I!" Turned out he was using someone else's notes. The audience roared and my students were impressed with the sincerity of my instructions to them about asking for explanations without embarrassment. Twenty years later, I got an email from one of my old JPC students reminding me of the incident and saying that it had stayed with him all these years.

2. **Reality Trumps Theory.** No matter what the textbooks say, no matter what's in the journals, and no matter what the experts say, focus on the actual situation you are facing. Don't let generalities and customary assumptions block you from seeing the real-world details of the problem you are trying to solve.

   In my statistics classes this week, I've been showing students some classic errors of the application of statistical methods. Here's a screenshot of one of the exercises in goodness-of-fit calculations:



QM213 HOMEWORK WEEK 14 PART 4 -- 5 PROBLEM SHEETS + ANSWER SHEETS

14-4E ESP Experiment Gone Bad -- answers

Some ESP researchers are testing a subject by having her guess whether a coin that is being tossed by an experimenter but which is hidden from the subject is heads or tails. There are 1,000 tests in the experiment. The subject's right and wrong guess frequencies are shown below. Test the hypothesis of randomness.

Guess	Observed	Expected
Right	498	500
Wrong	502	500
Total	1000	1000

H0: random
H1: not random

P(H0): 0.899343 ns
Conclusion: No signficant deviation from chance alone.

Not satisfied with this result, the experimenters take a close look at the 1,000 detailed results. They realize that the sequence from trial 86 to trial 391 (shown in red) seems to have a long run of correct guesses, so they test the goodness-of-fit for those selected data alone. What do they find?

Trial	RAW DATA
1	RIGHT
2	WRONG
3	RIGHT
4	RIGHT
5	WRONG
6	RIGHT
7	RIGHT
8	WRONG
9	WRONG
10	WRONG
11	RIGHT
12	WRONG
13	RIGHT

Guess	Observed	Expected
Right	226	153
Wrong	80	153
Total	306	306

H0: random
H1: not random

P(H0): 7.05E-17 ***
Conclusion: AHA! The experimenters are ecstatic! Proof that ESP exists!!! P << 0.001***

What's wrong with the experimenters' reasoning?

They ARE NOT USING A RANDOM SAMPLE. They deliberately picked an unusual run of right answers and pretended that these were random data. They're not random: the other data had much lower chance of being included than the run of data that supported the experimenters' assumptions. The assumptions of the chi-square goodness-of-fit test are NOT being met. This isn't science, it's propaganda!

The problem shows how investigators can search out deviant patterns (in this case, I made up an example in which there are 306 values with an unusually high proportion of right answers our of a total of 1,000 observations that on the whole don't deviate from random expectation) and then delude themselves into believing that their deliberately selected data are a random sample. It doesn't matter if their arithmetic is right: the assumptions of the analysis are not met, and the results are rubbish. Reality trumps theory. (You can download the actual exercise as an Excel XLSX file here.< file: 081_esp.xlsx >)

In class, I pointed out that selection bias< http://skepdic.com/selectionbias.html > can ruin the validity of statistical analysis. For example, if an unsophisticated, uneducated grocery clerk is instructed by his boss to show that their oranges are bigger than their competitor's oranges, the poor clerk may deliberately or perhaps unconsciously select the biggest oranges in his employer's bins and the smallest oranges in the competitor's bins. Any attempt to conclude something like "The probability that the observed chi-square value or larger could occur by chance alone if the null hypothesis of equal orange sizes were true is only 10^-17" fails on the issue of "by chance alone."

On a related note, readers may like the lecture on "How to Solve Technical Problems"< http://www.mekabay.com/courses/academic/jac/TSP/2_prob.ppt > from my old JPC course on The Art of Technical Support< http://www.mekabay.com/courses/academic/jac/TSP/index.htm >. Some of the principles articulated in that course are

- Get the global picture
- Distinguish observation from assumption
- Distinguish observation from hearsay
- Distinguish observation from hypothesis
- Challenge your hypothesis.

3. **Better Crazy than Boring.** This has only a little to do with information security but a great deal to do with life in general. I believe that being unpredictable in one's thinking and behaviour is an excellent life habit. Refusing to allow oneself to fall into rigid patterns of thinking and behaviour can lead one to novel perceptions and creative solutions.

   From a security standpoint, being unpredictable in one's monitoring and configurations deprives the attacker of a repeatable, predictable target. Uniformity may be helpful in many circumstances, but adapting to the particulars of a specific network or system can also be helpful.

   Being a bit crazy can enliven our teaching, our professional lives, our marriages, and our lives in general. For example, when I teach, sometimes I change my accent to keep the students awake; I'll switch into Russian, Indian, French, German and various sorts of British accents to the amusement of my students – who then don't fall asleep due to their 05:00 physical training exercises (most of our students are in the Corps of Cadets< http://www.norwich.edu/campus/together.html > at Norwich). As for my wife and I, we never know what the other is going to do or say. Just this week Deborah came home late while our dogs were away; since the two doggies routinely clamber into Deborah's car when she arrives, I did so instead to much laughter. After 30 years together, we still laugh with each other every day.

* * *

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/ >

* * *