Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Digital forensics must come of age

Recent decisions and views expressed by members of the judiciary and rulings of US courts seem to be bolstered further by a newly released report from the National Academy of Sciences titled "Strengthening Forensic Science in the United States: A Path Forward". This report includes as findings, thing like:

- Forensic science ... research, education, and training lack strong ties to our research universities and national science assets.
- Forensic science research is not well supported, and there is no unified strategy.
- Oversight and enforcement of operating standards, certification, accreditation, and ethics are lacking in most jurisdictions.
- Laboratory reports generated as the result of a scientific analysis should (but usually don't) contain, “methods and materials,” “procedures,” “results,” “conclusions,” and, as appropriate, sources and magnitudes of uncertainty in the procedures and conclusions.
- Practitioners have insufficient education and training to do their jobs appropriately.
- Forensic scientists and laboratories tend to work for prosecutors and law enforcement and methods as well as results are often biased in favor of the prosecution.
- Forensic laboratories tend to be uncertified and do not participate in cross-laboratory certifications or other calibration processes.
- "Homeland security" ended up being an emphasis area of the report. Politics...

The list goes on and on, but to summarize in simple terms, independent, unbiased, science-based forensics research and practice to defined standards must be put in place if forensics is to be reliably used as part of legal decisions.

Digital forensics as a microcosm

While the National Academy report more or less ignored the real issues in digital forensics, I have spent considerable time and effort in this area, and I certainly agree with the general conclusions of the National Academy when it comes to the digital forensics arena. The state of the art, and the state of the practice in digital forensics is not good.

In case after case, I have faced supposed "experts" that not only lack specific knowledge of the things they opine on, but make statements that are simply not true, draw conclusions that are not justified by the facts, write reports that fail to indicate the basis for their statements, don't reveal how they came to conclude what they conclude, don't indicate anything about methods or process, and don't indicate any notion about the reliability or science behind what they do. In some such cases, the experts apparently refused to sign their reports and submit them to the courts after being challenged on what their reports said.

The High Tech Crime Investigations Association, and other similar groups, seem to want to

start certification programs, but they don't allow membership or participation by those who don't follow their code of ethics, and their code of ethics excludes work for criminal defendants. And in a recent study of how their members regard the processes they use to do their jobs, there was substantial deviation about how to do those jobs, including steps that some indicated must be taken and others indicated must not be taken. This means that non-uniform practices supported by and favoring the prosecution and excluding others from participation, are embedded in the professional societies that claim to host those working in the digital forensic sciences.

And it gets worse. There is precious little in the way of a theoretical base for digital forensics, and where there is a basis, the theory is rarely applied in practice. That US National Institute of Science and Technology (NIST) has a process for testing and certifying hardware and software for digital forensics, but it is essentially limited to the ability to make a true copy of an original disk and the ability to search for a string within an image. While this is certainly something critical to be able to do properly, it is nothing like comprehensive in dealing with legal matters when digital evidence is in play.

Where to go from here

The NAS report has a section called "An Emerging Forensic Science Discipline: Digital And Multimedia Analysis" which may start to characterize the state of the situation. Emerging as in not yet emerged, discipline as in not really a science yet. And "analysis" is only a small part of the overall set of challenges faced in the digital forensics arena.

Digital forensics as a field has little structure, little science, and inadequate research and educational resources. There are few Masters level educational programs and the Ph.D. programs can be counted on less than the fingers of one hand. Training courses tend to be vendor training on the use of their tools and don't include much in the way of applying those tools to legal matters. In order for this to change, we need a serious national level effort to build the scientific base necessary to support digital forensics, and the educational base needed to support that scientific base. That means funding for university programs by government, and rigorous peer reviewed scientific publications associated with professional societies like the IEEE, ACM, and IFIP. It means many more conferences, the development of standard research methodologies, and - lest we forget - the notion that results should be confirmed by independent repetition of experiments by independent experimenters.

If this sounds like "real science" (as opposed to computer science), you are getting the idea. Real science has been desperately needed in the computer security arena for decades, and in the digital forensics arena since the first case involving a digital computer went to court. But while computer security, as a field, has a feedback mechanism that punished the inept, the legal system has a tendency to punish the innocent when forensic science is skewed and when non-scientific informaiton is presented as science.

So that's where we need to go from here. Toward real science in the information protection arena, and more specifically, in the digital forensics arena. Will we be able to do this in the foreseeable future? Only time will tell.

