Frauds, Spies and Lies:
A Little Treasure from Fred

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Fred Cohen, PhD is famous all over the world for his distinguished contributions to information security. His doctoral thesis on computer viruses is still cited as one of the most influential books in the field and he has taught innumerable university and industry courses on networking, cyber threats and defenses, security architecture, viruses, digital forensics and deception techniques and countermeasures. His Web site < http://all.net > is popping with interesting articles, course materials, and lectures. He is also an accomplished "Red Team" leader (penetration tester) with many years of hands-on experience in simulating malicious deception to test client security systems and procedures.

Recently Dr Cohen sent me a review copy of one of his books, _Frauds, Spies, and Lies and How to Defeat Them_ (ISBN 1-878109-36-7). At 234 pages, it's a delightful read, and I went through it pretty much in one session with much enjoyment.

The book is based on a course Dr Cohen has taught for some years about deception techniques and countermeasures. It begins with an extensive glossary of fraud and deception techniques, moves on to elicitation and intelligence (the methods used by government professionals), discusses counterintelligence methods, and finishes with a review of how to resist fraud personally and organizationally.

The book is full of good-humored comments such as "The casual reader might want to read only chapters 1, 2 and 6…. Government types might want to read the whole book. My graduate students had better read the whole book and everything on the Web site. The final is Tuesday."

Chapter 2 defines and describes 256 (if I counted right) distinct, named types of frauds, ranging from financial frauds through Internet-based schemes and ending with analyses of political machinations and propaganda techniques. Picking at random from this fascinating list, here is the entry (2.6.2.4) on phony job interviews:

>Some folks who want to get information on a company will arrange to get a job interview by applying for job with a fake resume. In the interview process they will ask questions and get tours of facilities that they can then exploit for the information on what is where, to plant a surveillance device, or to leave an explosive if sabotage or extortion is their goal.

Chapter 3 looks into the psychological underpinnings of deception and provide many references for further reading. Here is the beginning of a interesting section (3.11.2) on opportunistic fraudsters:

Opportunistic fraudsters are said to constitute about a third of all employees. They usually take little things here and there, but unlike most employees, they may go to extremes. They don't try to think up new frauds all the time, but rather they encounter system quirks and once they accidentally or 'legitimately' get around the system, they decide to do the same thing for advantage or quote compensation".

Dr Cohen then gives as an example a situation in which such an employee loses the receipt for a taxi ride on a business trip. The fraudster copies the real taxi receipt and makes some changes to re-create the lost paper-- no theft involved. However, it becomes tempting to use the same technique again, this time for fraud.

After reviewing the methods used by spies (Chapter 4), Dr Cohen provides many practical measures in Chapter 5 for evading the clutches of professional spies. For example, he suggests "misunderstanding" a leading question and replying with nonsense such as "I had one of these when I was a kid." (section 5.4.1.6)

Chapter 6 includes an extensive list of recommendations for reducing susceptibility to fraud, including corporate policy guidelines and good advice for individuals.

In summary, this is a wonderful book for anyone interested in security, psychology of crime, politics and clear thinking. I'm seriously considering incorporating it into my graduate program in information assurance as required reading in the Human Factors seminar.

Anyone wanting to buy a copy of the book can get it easily at < http://asp-press.com/ > for $29.00 – a real (ahem) steal!

Good one, Fred!