A Reading List

Computer security is not merely a technical field. Knowing about people, and about societies, guides the application of the technical material. During this class we'll often refer to an eclectic collection of books that teach lessons we can apply to computer security. These are some we've referred to in past classes, plus a few of our favorites. Tom chose some, and Matt chose the rest. (You can probably figure out who suggested at least one.) In any case, we both recommend these.

Non-Technical Books

- Saul Alinsky, *Reveille for Radicals*, Vintage Books
  The classic analysis of organization for social improvement. Many of the techniques Alinsky discusses can be adapted to attacking systems—or defending them.
- Saul Alinsky, *Rules for Radicals*, Vintage Books
  How the Have-Nots can organize to change society. Like Alinsky's other book, the rules are applicable to computer security.
- James Bamford, *The Puzzle Palace*, Viking Press
  A book on the history of the NSA.
- Alfred Bester, *The Demolished Man*, Vintage Books
  The struggle between the killer Ben Reich, the 24th century's richest man, and Lincoln Powell, the police prefect with ESP, is like a cat-and-mouse game between an attacker and computer security folks. This classic science fiction book won the first Hugo for Best Novel. Bester was named the first Grand Master of science fiction.
- John Brunner, *The Shockwave Rider*, Ballantine Books
  A science fiction novel about a future in which data about everyone is stored in a ubiquitous information network. Many of the terms used with malicious logic, such as virus, were first used here.
- James Burton, *The Pentagon Wars*, United States Naval Institute
  A study of how a group of reformers tried to test and improve some weaponry, and what happened. A wonderful and eye-opening description of bureaucratic in-fighting.
- Dorothy Denning, *Information Warfare and Security*, Addison-Wesley Publishing Company
  Good background on issues we discussed in class, nice presentation. Mentions some Matt Bishop guy.
- Jean Guisnel, *Cyberwars: Espionage on the Internet*, Plenum Press
  Written by a Frenchman, so an interesting non-US perspective.
- Niccolò Machiavelli, *The Prince*, Penguin Books
  Its study of rulers applies not only to princes, but also to organizations and environments in general.
- Eric Frank Russell, *Wasp*, Tor Books
  A science fiction novel in which a lone agent is dropped on an enemy planet. His job: cause chaos. He does.
- Neal Stephenson, *Cryptonomicon*, Avon Books
  Good discussion of World War II cryptography, and real world/wartime issues involving security of communications, *etc*. Great mathematical perspective.
- Neal Stephenson, *Snow Crash*, Spectra Books
  Okay, this one's more marginally computer security related, but it has a virtual reality interface figuring prominently into the plot, and deals with issues of networking through metaphor.
- Sun Tzu, *The Art of War*, Delta
  A classic text on warfare, many of its principles can be translated into cyberwarfare.
- Vernor Vinge, *Fire Upon the Deep*, Tor Books
  Superb science fiction book with computer security applications.
- Vernor Vinge, *True Names*, Tor Books
  First real cyberpunk book; Gibson got credit for this sort of work.

Technical Books

- Bruce Schneier, *Applied Cryptography*, Second Edition, John Wiley and Sons
  A comprehensive introduction to cryptography. The mathematics is basic, but the book presents sophisticated algorithms. It's also well written and easy to understand.
- Simson Garfinkel and Gene Spafford, *Practical UNIX and Internet Security*, Second Edition, O'Reilly and Associates
  An excellent book on UNIX security.
- Charlie Kaufman, Radia Perlman, Mike Speciner, *Network Security: Private Communications in a Public World*, Prentice-Hall Publishing Company
  Excellent examples of DES and I think probably the most readable textbook I've found on the subject, without skimping too terribly much on details. I like their treatment of the subject matter a lot.