

## Discussion of *The Cuckoo's Egg* by Clifford Stoll

1. Did you like the book? If so, what was your favorite part of the book? If not, why not?
2. The author has a personal struggle with right and wrong. He has some strong suspicions about governmental agencies, but finds he and the agencies are on the “right” side trying to catch the spies. While watching the spy roam around computers, he struggles with whether he should stop the spy now or watch and track so the spy can be caught. How do you think you would have acted in his situation?
3. How has computer security changed in the 18 years since the book was written?
4. On p. 35, Stoll writes, “Depending on how you looked at it, our data was worth either nothing or zillions of dollars. How much is the structure of an enzyme worth? What’s the value of a high-temperature conductor? The FBI thought in terms of bank embezzlement; we lived in a world of research.” Is computer hacking “wrong” even if there is no direct monetary loss?
5. On p. 48, Stoll writes, “If everyone used the same version of the same operating system, a single security hole would let hackers into all the computers....The variety of software meant that no single attack could succeed against all systems. Just like genetic diversity, which prevents an epidemic from wiping out a whole species at once, diversity in software is a good thing.” In the 20 years since this book was written, software has gotten a lot less diverse. The number of widely used operating systems and Internet browsers has gone down. Does this mean we are living in an even less secure world?
6. On p. 59, the author writes, “Most personal computers satisfy the needs of their owners, and don’t need to talk to other systems.” Today, most people use personal computers to send email and surf the Internet in addition to word processing, etc. What’s the significance of this change?
7. On p. 65, Stoll writes, “For the first time, I realized that my civil rights actually limit what police can do.” Do you agree? Disagree? Stoll has taken a lot of flack over this and similar comments, since his book has been used as an excuse for ignoring civil rights.
8. All of the government agencies seem to be operating independently and are unwilling to share information with each other (e.g., p. 116). Have we learned anything? This happened in the months and week before 9/11 as well.
9. Stoll details a lot of information about computer passwords (as on p. 250). This is information I wish I could convey to everyone I teach about computers. If you use a word that is in a dictionary, without the addition of a number or upper and lower case letters, it can be guessed by a program. Did any of you learn things about computer security that you didn’t know while reading this book?
10. On p. 288, Stoll writes, “I learned what our networks are. I had thought of them as a complicated technical device, a tangle of wires and circuits. But they’re much more than that – a fragile community of people, bonded together by trust and cooperation. If that trust is broken, the community will vanish forever.” Comments?

11. On p. 302, Stoll writes, “after sliding down this Alice-in-Wonderland hole, I find the political left and the right reconciled in their mutual dependency on computers. The right sees computer security as necessary to protect national secrets; my leftie friends worry about an invasion of privacy when prowlers pilfer data banks. Political centrists realize that insecure computers cost money when their data is exploited by outsiders. The computer has become a common denominator that knows no intellectual, political, or bureaucratic bounds”. Reactions?
12. Does the need to keep computers secure and to instill shared values in our online communities ever justify the government’s violation of the civil liberties of individuals?
13. A quote from Cliff Stoll that came out after the publication of the book: “Our civil rights – including free speech and privacy – must be preserved on the electronic frontier. At the same time, we must respect each other’s rights to privacy and free speech. This means not writing viruses, breaking into another’s computer, or posting messages certain to cause flame wars. Just as important, it means treating each other with civility, respect, and tolerance.”
14. On p. 323, the author concludes:

The monster is still out there, ready to come alive again. Whenever someone, tempted by money, power, or simple curiosity, steals a password and prowls the networks. Whenever someone forgets that the networks she loves to play on are fragile, and can only exist when people trust each other. Whenever a fun-loving student breaks into systems as a game (as I might once have done), and forgets that he’s invading people’s privacy, endangering data that others have sweated over, sowing distrust and paranoia. Networks aren’t made of printed circuits, but of people....Thousands of people trust each other enough to tie their systems together....Like the innocent small town invaded in a monster movie, all those people work and play, unaware of how fragile and vulnerable their community is. It could be destroyed outright by a virus, or, worse, it could consume itself with mutual suspicion, tangle itself up in locks, security checkpoints, and surveillance; whither away by becoming so inaccessible and bureaucratic that nobody would want it anymore.

Any comments in reaction to this conclusion?

15. Has anyone had experiences relevant to this book that you’d like to share?
16. Are there any questions you would like to ask?