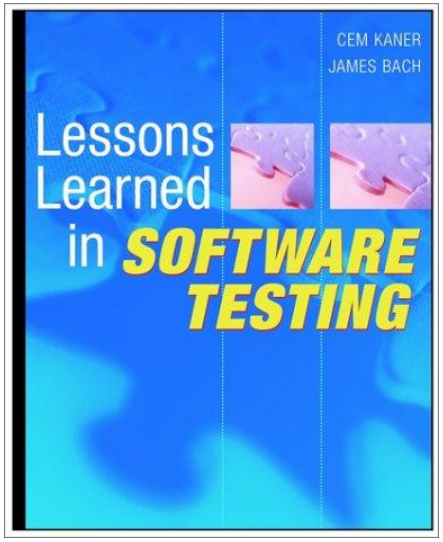
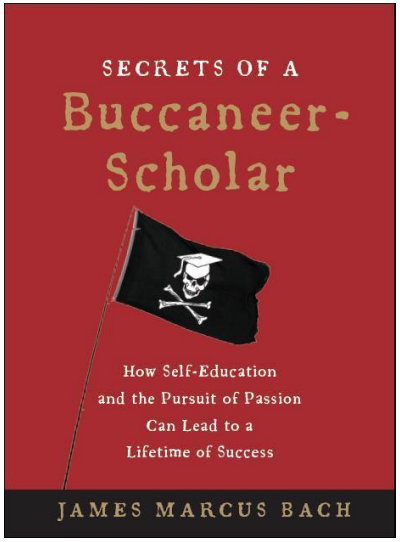
Why is most software not designed with security in mind and never will be?

James Bach

I am a tester and a programmer. Mostly a tester.

I wrote a book on testing and a book on self-education.





I enjoy deep testing, including occasional security testing and other "hacking…"

Wall Street Journal
May 10, 2002

"The states announced Sunday night that they would call Mr. Bach to show how to build custom versions of the Windows operating system.

Yesterday, the judge expressed displeasure, appearing visibly angered by the states' 11th-hour complications."

The Elements of the Security Problem

- **Ambition** to create new technology.
- **Old technology** that forms the basis for new.
- **Problems** hiding in technology.
- Incentives **to find** the problems.
- Incentives **to ignore** the problems.
- Difficulty of **finding** problems.
- **Cost to fix** the problems.
- **Cost of bearing** the problems.

Security Requires Crazy Thinking

- **Normal:** Obscure bugs aren't important.
- **Crazy:** Nothing is obscure.

- **Normal:** Users want it to work.
- **Crazy:** Users are working to make it fail.

- **Normal:** Programmers cause bugs.
- **Crazy:** Attackers seen as creating bugs.

“No user would do that.”

“No user I can think of, who I like, would do that on purpose.”

James Bach

james@satisfice.com

http://www.satisfice.com

@jamesmarcusbach