Deconstructing the myths behind the full-disclosure debate.

The term "full disclosure" is marvelously ambiguous, and therein lies much of the problem. It essentially means to "widely disseminate as much information about system vulnerabilities and attack tools as possible so that potential victims are as knowledgeable as those who attack them." Admittedly, this concept has a certain appeal. But where does this "information" to disseminate come from?

Developments in human technology follow a consistent pattern: a basic researcher (of which there are precious few) discovers a new principle; an engineer (of which there are a few more) builds a tool that applies the principal; and non-specialists (there are a bunch of these) use the new tool. Long before the term "script-kiddie" came into vogue, a small core of gurus was recognized as responsible for discovering most security bugs. A larger group of skilled programmers then wrote programs to exploit these bugs, releasing them to the greater population of hacker-wannabes.

Having discovered that they can attract huge amounts of attention by throwing rocks at Windows, so-called security professionals are increasingly the ones fulfilling both the research and the application stages. Sadly, the shortest path to computer security fame seems to lie more in providing candy to children than in breakthroughs in dental hygiene. The concept of full disclosure is, indeed, ambiguous, serving as a politically correct shield behind which all manner of self-serving behavior can be justified. It's far too often used to rationalize shortsighted information releases that benefit the announcer to the detriment of the entire Internet community.

Marcus Ranum could hardly have chosen a more provocative venue to

launch his harsh criticism of full disclosure than the keynote session of last year's Black Hat convention. In a speech entitled, "Script Kiddiez Suck," he denounced several myths about full disclosure, arguing that it has created armies of hacker-wannabes while doing nothing to improve the state of security. He specifically stated that "many of the vulnerabilities being disclosed are researched and discovered for the purpose of being disclosed." This is also my observation. How many reputations have been launched under the guise of full disclosure? Is this really to our benefit, or is it actually to our detriment?

@stake/L0pht researcher Weld Pond responded to Ranum's keynote with a two-page ZDNet op-ed that employed the word "free" three times. Praising Ranum's courage for raising an important issue, Pond then proceeded to slap him upside the head, claiming that without full disclosure, "[script-kiddiez] would be replaced with something far worse: attackers who can uncover their own vulnerabilities, or have the connections to pay for them."

Foundstone's Stuart McClure and Joel Scambray wrote in their InfoWorld column, "The way to fight a regime of terror is to fight it with information- via full disclosure." These pundits offered no evidence to substantiate this significant claim. They may be right, but when evaluating their argument, keep in mind that their pocketbooks have benefited substantially from the sale of their popular book, Hacking Exposed, in which numerous exploits are discussed in detail.

Human nature seems to turn every question into a binary. This makes debate a lot more fun, but it's the lazyman's way to solve a problem. Instead of striving for the optimum compromise, just choose one of the poles. You won't have to think hard, and you have the added satisfaction of moral superiority. Cloaked in black leather and tattoos, the self-righteous' attempt to turn full disclosure into a First Amendment issue

misses the point. Instead, we need to ask what activities will produce the greatest common good. Donn Parker is fond of saying that our profession is to a real science as alchemy is to chemistry. Is scientific research available on the subject of disclosure? If there is, it's certainly not enough to substantiate the claim that disseminating high explosives is actually reducing the rate of bombings.

The true costs and benefits of disclosure can only be understood in economic terms. Unfortunately, neither side of this debate has taken advantage of the research discipline that is designed to answer such a question.

My hypothesis is that both "full disclosure" and "no disclosure" are terribly costly, and that the optimum benefit to humanity is some difficult-to-determine compromise position. But I'm not an economist, either, and I guess alchemy is just more fun than real science.