Locks and Full Disclosure

Bruce Schneier
Counterpane Internet Security

The full disclosure versus bug secrecy debate is a lot larger than computer security. Matt Blaze's article on master-key locking systems in this issue (page 24) is a case in point. It turns out that the ways we've learned to conceptualize security and attacks in the computer world are directly applicable to other areas of security—like door locks. But the most interesting part of this story is that the locksmith community went ballistic after Blaze published his research on master-key lock vulnerability.

The technique of creating a master key from other keys was known in the locksmithing and criminal communities for over a century, but was never discussed in public and remained folklore. Customers who bought these master-key systems were completely oblivious to their security risks. Locksmiths liked it this way, believing that a system's security increases by keeping the general population from learning these vulnerabilities.

The bug secrecy position is a lot easier to explain to a layperson. If there's a vulnerability in a system, it's better not to make that vulnerability public. As the argument goes, the bad guys will learn about it. According to this position, the problem is more the information about the vulnerability and less the vulnerability itself.

This position ignores the fact that public scrutiny is the only reliable way to improve security. Several master-key designs are immune to the 100-year-old attack that Blaze rediscovered. But these locks are not in widespread use because customers don't understand the risks, and because locksmiths continue to knowingly sell flawed security systems. This is no different than the computer world. Before we routinely published software vulnerabilities, vendors would not bother to spend the time and money to fix vulnerabilities, believing in the security of secrecy. And because customers didn't know any better, they bought these systems, believing them to be secure. If we return to a world of bug secrecy in computers, we'll have 100-year-old vulnerabilities known by a few in the security community and by the hacker underground.

That's the other fallacy with the locksmiths' argument. Techniques like this are passed down as folklore in the criminal community as well as the locksmithing community. In 1994, a thief made his own master key to a series of safe-deposit boxes and stole $1.5 million in jewels. The same thing happens in the computer world. By the time a computer vulnerability is announced in the press and patched, it's already folklore in the hacker underground. Attackers don't abide by secrecy agreements.

This culture clash is happening in many areas of security. US Attorney General John Ashcroft is trying to keep details of many antiterrorism countermeasures secret so as not to educate the terrorists. But at the same time, the people—to whom he is ultimately accountable—are not allowed to evaluate the countermeasures, or comment on their efficacy. Security can't improve because there's no public debate or public education. Whatever attacks and defenses people learn will become folklore, never spoken about in the open but whispered from security engineer to security engineer and from terrorist to terrorist. And maybe in 100 years someone will publish an attack that some security engineers knew about, that terrorists and criminals had been exploiting for much of that time, but about which the general public was blissfully unaware.

Secrecy prevents people from assessing their own risks. For example, in the master-key case, even if there weren't more secure designs available, many customers might have decided not to use master keying if they knew how easy it was for attackers to make their own master keys.

I'd rather have as much information as I can to make informed decisions about security. I'd rather have the information I need to pressure vendors to improve security. I don't want to live in a world where locksmiths can sell me a master-key system that they know doesn't work or where the government can implement security measures without accountability. □

__Bruce Schneier__ is chief technology officer of Counterpane Internet Security and the author of over seven books on cryptography and computer security. You can subscribe to his free email newsletter, Crypto-Gram, at www.counterpane.com/crypto-gram.html, or contact him directly at schneier@counterpane.com.

1540-7993/03/$17.00 © 2003 IEEE