IS ENCRYPTION SAFE?

Encryption utilities are readily available and easy enough for even novices to handle. Win2000 and XP machines with NTFS-formatted hard drives even have encryption available as a right-click option in My Computer. But is today's encryption good enough to trust with your vital data?

In 1977, the U.S. government adopted the 56-bit DES (Data Encryption Standard), making it the de facto encryption algorithm for nearly all agencies. By the mid-'90s, the Electronic Frontier Foundation and others said the algorithm was no longer worthy to guard national secrets. In 1998, the EFF used its DES Cracker (costing less than $250,000) to crack DES in less than three days. In January 1999, the EFF teamed with Distributed.net to set thousands of PCs on the problem at once, resulting in a crack time of 22 hours. The government got the hint, and in 2001 selected Rijndael, an encryption algorithm with as many as 256-bit keys, as the new AES (Advanced Encryption Standard).

How safe is the encryption on your desktop? If you're only using a password to protect your Word and Excel files, this is merely converted into a 5-byte code. Guess the code (the odds are one in 1.5 trillion) and you're in. AccessData (www.accessdata.com) sells Distributed Network Attack ($249), essentially a brute force tool designed to crack such passwords.

The EFS (Encrypting File System) in Win2000/XP uses 128-bit keys. Rent-A-Hacker's John Klein says his organization has cracked EFS a couple of times to help clients who have locked themselves out of important files. Ultimately, he says, you can crack any encryption scheme.

"Years ago, we heard that this or that particular algorithm would take X billions of years to crack on a Cray," says Klein. "But the Cray then is my desktop now. A seven-character alphanumeric password is crackable in less than three hours using brute force tools, and the typical password used by most people and almost all home users is crackable in less than three minutes. I just pre-seed the dictionary with kids' names, dogs' names, addresses, phone numbers, and invariably I'll come up with it in three minutes. Now, PGP still hasn't been cracked and probably won't be for many, many years, but if I have direct access to the computer so I can copy the files off and get to work on them, eventually someday I'll crack them."

Benjamin Jun, vice president of Cryptography Research, which built the DES Cracker, says, "Most of the problems we see are not people breaking crypto. It's more things like buffer overflow attacks or other low-hanging fruit that provide system access."

ONLINE WITH TWO TOP HACKERS

Kelvin "Mercs" Wong understands black hats. He was one before turning to the good side. According to John Klein, president of Rent-A-Hacker (www.rent-a-hacker.com), Wong has written (and subsequently deleted) automated software capable of turning fleets of improperly protected systems into zombies under his command–just to prove it could be done.

/dev/null, when not making a living as a white hat, spends his hours at Attrition.com helping those who genuinely want to learn for learning's sake. On the other hand, his Going Postal writings hilariously lambaste the ignorant masses that ask him for help with defacing sites or digging into their girlfriends' mail accounts.

Both hackers granted CPU email interviews and offered some honest insight into the hacking world.

CPU: Why do people, or you in particular, hack?

Wong: To me, hacking itself redefines the conventional way of learning. It is exciting, yet frustrating at times. The desire to hack springs from the psyche of man to learn and the rebellious nature of our adolescence. This is one of the many reasons why we're seeing an increase in teenagers wanting to learn to hack. The desire is there, but rather, you must question the motive(s) behind it. The reasons are many. They hack because they can; they hack for political agendas (i.e: hacktivism), personal gains, revenge, corporate espionage, etc. The list goes on.

The thrill of avoiding being noticed, seen, or caught is like an adrenalin rush that most hackers find "exciting." It is also the whole process of learning and attempting to "break" into the system that thrills them. Some have a clear objective, some don't; the obtaining of classified information and software, the rebellious nature that we have within us to try to circumvent the law, etc. The reasons as mentioned earlier are many and vast. Some do it to gain popularity and media attention, some for money, and some even to proclaim their love for the girl that they've lost or could have never gotten.

/dev/null: It's the creativity. It's having to think in unusual ways, having to play detective, having to find the unexpected paths to get in

"In essence, being a 'HACKER' has a lot more to do with the mentality than it does how the MENTALITY manifests itself."

- /dev/null, white hat hacker

and find information, making computers do things they weren't intended to do. I love that.

What got me into the Internet 12 years ago was this revolutionary way to communicate with people all over the world, and the opportunity to explore what felt like a new frontier. I'm still exploring. The more the Internet develops, the more interesting it is to me. As more tools come out, there are more toys to play with, to take apart, to find out what makes things tick. It's exciting. I love being part of the hacking scene now.

CPU: What are the pros and cons of being a hacker?

Wong: Pros vs. cons are raised in every job that you do. Benefits include the "legality" of hacking. It is part of the job and you get paid for doing it. However, often times, you are tempted to "poke" around the machine, to see what you can find. There is a very fine line, and we're often stuck in the gray area. I often remind myself that despite all that, I am a professional now and that I take pride in my work. The key to all this is restraint. Cons include time constraints to make the deadline and the writing up of reports and assessments.

/dev/null: The biggest pro is that I get paid for doing something I really enjoy. I get to challenge myself and be creative every time I go to work. I get to figure things out and play with great toys. More importantly–perhaps most importantly–I have a job that drives me to constantly learn. I can't think of anything more exciting than always learning new things.

The cons, well, to me there are few cons, other than the standard problems that any consultant has to deal with (long hours sometimes, irregular periods of work and rest, etc). I really like what I do. The thing that a lot of people might have to bear in mind about being a professional hacker comes back to public perception: People will be unsure whether or not you can be trusted. Your ethics have to be above reproach. There have been too many people who've worked as security consultants during the day while breaking into sites illegally at night. When they get arrested, it makes all of us look bad, and people like that merit very little respect from the community.

CPU: Kelvin, you should know more than anyone: Can a black hat ever be 100% reformed for life?

Wong: I would like to mention for the record that several years ago an article was posted regarding Christopher Klaus, founder of Internet Security Systems, [that he] was a cracker. I think that anything is possible. This includes a black hat hacker becoming totally legit. I am living testimony of that. However, I do admit that sometimes I do feel tempted to hack illegally, but now that I've grown in maturity and am wiser, I always weighed both the benefits and shortcomings of my actions and the consequences of that result. This deters me from doing so. Theoretically, white hat hackers are meant to be strictly legit in all their assessments. However, sometimes you must question the ways in which you do obtain private exploits to conduct security-penetration tests. Isn't trading or obtaining private exploits from other black hat or underground hackers a contradiction to all that they stand for? But I guess that's the business world. There is a very fine line drawn between the white hat and black hat; I believe that the majority of us fall into the 'gray' area category.

CPU: Null, you're regularly approached at Attrition by script kiddies and other "mouthbreathers" who try to enlist you in illegal activities. Why do they think and behave as they do?

/dev/null: Think about it this way: You are a 15-year-old kid smart enough that school isn't much of a challenge. You're chock full of frustrations and anger at pretty much anything and everything. Now you find a place, a medium, where you know more than your parents, your teachers, and half the people using it. You're 15 and you know more than an adult about this technology. You feel like a god. What better way to prove how much more you know, how much smarter than everyone else you are, than to successfully attack someone else's computer? It's a power rush. It's a sense of accomplishment. There is danger, but it's not the likely-to-kill-you sort of danger that comes with driving really fast or doing massive amounts of drugs, and it's not the damaging-to-social-status sort of danger that comes with taking chances with peers. It is a rebellion, yes, but not so much against authority–these kids aren't thinking about getting caught. They're not thinking about cat-and-mouse games with the cops or challenging their parents. It's a rebellion against the idea that a teenager has no power and no ability to affect his world.

"I've always been CURIOUS about government/military sites. If you asked why, I really wouldn't know how to answer you. Perhaps it's the many American TV MOVIES we've seen on the topic of hacking. Maybe it's the quest for highly confidential files or high-profile sites."

- Kelvin Wong