TODAY's HACKER:

HEAVENLY OR BOUND FOR HELL?

Spotlight Contents:

Graphics & Design by Ginger R. Riley & Jason Codr

"Imagine what would happen if you were head of the local PTA, active in your church's youth group, and helped teach kids at the Y," muses /dev/null, a white hat hacker and staff member at the popular hacking site Attrition.org. "One day the police get an anonymous tip that you're a key figure in an international child porn ring. They confiscate your computer, and there are tons of files of explicit photos. Your reputation is stained forever, even if you can prove in court that it wasn't you; it was someone who broke into your computer. So how bad can a hack get? Well, how bad can you imagine it getting?"

That's the hard news—the worst case scenario Hollywood, security products companies, and those who discuss the imminent cyberterrorist threat might have you believe is the norm in the world of hacking. The good news is that with a modest amount of precaution, small companies and everyday users are fairly safe from hackers.

"True hackers very, very rarely do damage," says John Klein, president of Rent-A-Hacker (www.rent-a-hacker.com). "They can write their own code and think in creative ways that can't entirely be copied through training. Often, their goal is just to prove a theory."

If true hackers are the Van Goghs and Dalís of their trade, script kiddies are their back-alley, spray paint-wielding counterparts. These are generally bright but unmotivated teens that crave praise for defacing Web sites or launching minor DoS (denial of service) attacks on unsuspecting businesses.

So, should you worry about hackers or be asking them for help?

THE HACKER'S MIND

The meaning of "hacking" has drifted over the decades. In the '60s and '70s, student programmers at universities often had to reverse engineer code to continue their educations because no software alternatives were available. Today, "hacking" generally refers to unauthorized access to a computer or network. Because this tends to be illegal and sometimes destructive, hackers have been branded as dangerous miscreants little better than terrorists.

This sentiment is largely based on media hype and the general public's lack of technical understanding. Without question, a large population of script kiddies hell-bent on causing damage exists, but far less frequent are the truly knowledgeable, seriously dangerous hackers who use their talents for revenge, embezzlement, or other nefarious ends.

At the opposite end of the spectrum are "white hat" hackers who abide by the law (in spirit at least), often selling their skills to public/private organizations to help guard against "black hat" hackers. Some prefer to use the terms "hackers" and "crackers." Hacker and open-source advocate Eric S. Raymond says, "Hackers build things; crackers break them."

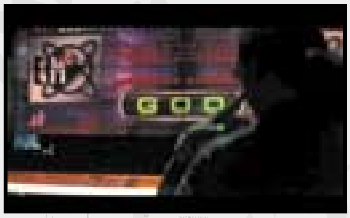
"In essence, being a 'hacker' has a lot more to do with the mentality than it does how the mentality manifests itself," says /dev/null. "Franklin was a hacker. da Vinci was a hacker. That's what it's all about—the curiosity, the experimentation, the inquisitive mind, the creativity. Most of the older hackers I know don't frown on the younger hackers so much as they frown on the media portrayal of hackers and the proliferation of the obnoxious kiddies who can use point-and-drool tools to be destructive. That's not what hacking was all about, and I don't blame them for their frustration at all."

Can a once-mischievous young hacker be trusted as a responsible adult security expert? John Klein thinks so. He made Australian Kelvin "Mercs" Wong COO of Rent-A-Hacker. Wong started learning to hack in 1997 at 16. Klein says Wong's father was a traveling executive who often left his son unsupervised with powerful Sun computers and loads of available Internet bandwidth. Before long, Wong had hacked NASA, the U.S. Army, and the U.S. Department of Agriculture, landing himself on Uncle Sam's watch list.

"The first machine that I ever hacked was part of the Defense Information Systems Agency," says Wong. "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. Back in 1997, security on gov/mil sites was shocking. A simple, common

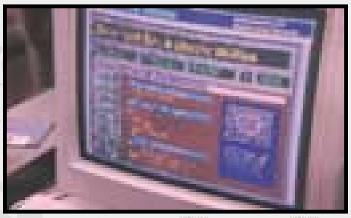
HACKING ON CELLULOID

Hollywood loves a hack, but do mega-budget films do justice to hacking and cracking? We look at five of the biggest flicks in the field to find out.



"Hackers" (thumbs down):
Not even Angelina Jolie's lips and occasionally witty dialogue saved this 1995 teen-cyberthriller from the ridiculous, nearly hallucinogenic depictions of server directories as skyscrapers and viruses as Pac-Men and rabbits munching on bytes of data. The movie gets points for drawing a line between well-intentioned vs. truly malicious hackers.

"Independence Day"(thumbs down):
Any alien race dumb enough to neglect installing a firewall against software viruses deserves to crash and burn. Then again, so does this ludicrous, 153-minute barrage of scale-model pyrotechnics. Apple missed the boat by not advertising its OS is wireless ETware-compatible.



"The Net" (thumbs down):
Should we take issue with a Whois lookup yielding someone's photo or the idea that one virus can melt any server system just by pressing the ESC key? (Note to bad guys: Run antivirus software.) The movie was, however, really the first major '90s flick to meld people's fears about network technology with general conspiracy paranoia.

"Swordfish" (thumbs up):
Forget about Halle Berry (if you can). The critics hated "Swordfish," and Travolta's evil hipster performance is cringe-worthy. Nevertheless, Hugh Jackman makes a convincing former black hat, and the hacking technology–if you forgive the sculpture of flat panels at his workstation–is pretty respectable.

"WarGames" (thumbs up):
Could a phone-phreaking, grade-changing Matthew Broderick really hack the Pentagon and inadvertently launch World War III? In 1983, government computers were quite hackable, but not even the DoD would lump nuclear systems software in with a bunch of games. "WarGames" did pioneer the hacking subgenre on the silver screen, and in a campy way, it's still fun to watch.

exploit, downloadable on the Net, could be easily used to gain access and exploit the machine for full control (root/superuser access)."

Faced with turning 18 and being eligible to rot away in jail, Wong donned a white hat, became a security consultant, and ultimately wound up topping the roster of 300-plus freelancers at Rent-A-Hacker.

"Why do hackers hack?" asks John Klein. "Our company helped conduct a survey covering roughly a couple thousand hackers. We found that about 64% responded 'because they're bored.' Ask Kelvin why he decided to take up hacking and successfully hack the U.S. Department of Agriculture. The reason is because he had nothing better to do that day."

THE BEST DEFENSE

According to the Computer Emergency Research Team (www.cert.org) at Carnegie Mellon University, 401 hacking incidents were reported in 1991 vs. 52,658 in 2001. The first half of 2002 alone has yielded 43,136 incidents. About the best defense typical home users have is running at least one reputable antivirus program that's assiduously updated, a firewall (if not a hardware firewall via a router, then at least a software firewall), and, in extreme cases, unplugging from the Internet whenever possible.

> "HACKERS build things; CRACKERS break them."
>
> – hacker and open source advocate Eric S. Raymond

The task is more difficult and expensive for businesses, but many companies have more to lose. Rent-A-Hacker markets to

HIGH ON CRACKZ

Why spend $50 on the latest game or $500 on a business app when you can snag it off the Web free? That seems to be what software pirates think when uploading/downloading files to/from specialized sites that typically fall under the term "warez," as in software(s).

According to the Business Software Alliance, piracy-related losses for the software industry totaled $11 billion in 2001. Jason Allen, antipiracy investigator for the Interactive Digital Software Association, says pinpointing losses from illegal downloads vs. disc duplicating is difficult, but he estimates Internet-related losses in entertainment apps alone is "in the billions."

"We believe that the Internet piracy problem is the biggest growth area," says the BSA's Bob Kruger, vice president of enforcement. "Whatever the percentage of losses is attributable to piracy is today, it'll be a higher percentage tomorrow. It's a triple whammy: There are more people online, programs are easier and faster to download, and culprits are more difficult to identify and pursue."

Warez groups have their own subcultures based on content. "Appz" groups focus on applications, "gamez" on games, "serialz" and "crackz" on serial numbers and codes that can help unlock software, and so on. The BSA and other groups do a formidable job of knocking warez sites off the Web, but others spring up. Trying to find Web-based warez is likely to lead to dead links, porn-related pop ups, and wasted time. Most real-file transfers are done directly with FTP clients and IM apps.

Often, warez shows up online before retail versions hit store shelves. IDSA's Allen says prerelease "gold" copies are sometimes stolen or leaked by insiders or crackers occasionally pose as press reviewers to obtain advance copies. Money may be a factor, such as when the buyer is a large-scale disc duplicator. More often crackers are motivated by breaking software security and the ego boost of posting a new title first.

"Crackers will deconstruct the code of the game," says Allen, "and they'll look for the part of the code, almost like a chapter in a book, that deals with copy protection. They'll rewrite the book so that the copy protection is no longer included, and then they'll put it back together and republish it online."

Shutting down overseas warez operations can prove problematic, notes Kruger. Countries with low piracy rates often cooperate willingly, but countries such as Russia and China, where piracy rates are 87% and 92%, respectively, tend to be less cooperative. Kruger says several Southeast Asian nations are taking more active roles, however, perhaps because few IP-related companies will invest in an area where piracy goes unchecked.

U.S. sting operations occasionally capture high-profile crackers, but the offenders may not be the script kiddies you'd expect. The DrinkOrDie warez group made headlines last May when its leader, John "eriFlleH" (HellFire spelled backward) Sankus Jr. was sentenced to 46 months in federal prison. Sankus and more than 40 other crackers were netted in the 14-month, U.S. Customs Service-run Operation Buccaneer.

small- and medium-sized businesses, with hourly prices starting at about $170 to analyze weaknesses and suggest methods for patching them. That may be a bargain. /dev/null says his services once ran $2,500 a day plus expenses working for a company where he was fairly "low on the totem pole." Other hackers at the same company were commanding as much as $10,000 per day.

IBM's "ethical hackers" reportedly charge $15,000 to $45,000 for a single hack. This covers would-be attacks by a lone, relatively inexperienced hacker; a small team of experienced hackers; and a large team of determined experts. Asked if Big Blue is above seducing a client's janitor to complete a hack, Mike Bilger, global practice leader, IBM Security and Privacy Services, says it is up to the client to define the rules of engagement.

"We have done dumpster diving and other forms of social engineering, like being an imposter, gaining access to user IDs and passwords through the help desk and telephone centers—things like that. I mean, caller ID when you're sitting at the CIO's desk calling the help center can be a wonderful thing," Bilger says.

IBM trains its hackers from scratch, unlike some security consultancies. The ethical hacking effort started with recruits from IBM's research labs. It grew to include system administrators and college graduates. IBM trains them according to a rigorous and well-planned methodology.

"We will not hire ex-hackers," emphasizes Bilger. "We're not going to jeopardize our clients by bringing someone in that we don't feel comfortable with."

IBM takes this approach to earn the trust of its many Fortune 500-class clients. The military works similarly, using a blanket background check policy to deny anyone with a questionable hacking past. (Most government branches outside of the military do regularly employ hackers as consultants.) Klein says although you can teach a large amount of hacking academically, certain ingredients apply only to hackers who have honed their skills in real-life trenches.

"One of the key things you miss with training is the communication channels that hackers maintain," says Klein. "It's ever-changing and difficult to tap into. It's very hard to know what IRC channels to go to or what Web site to go to for information about what's really hot, right this moment. If you ask me what exploit is being used just within the last two days, I can tell you because I have guys who sit on IRC that are trusted by the hacker community because they're part of it and they know this information. But some guy sitting on a .gov address can't go flying into a hacker room and say, 'Hey, tell me what's hot!'"

"TRUE hackers very, very RARELY do damage."

- John Klein, president of Rent-A-Hacker

ARE YOU A TARGET?

If a malicious hacker is interested in your system, he's probably setting it up to become a zombie for a future DoS attack. Your Quicken files or love letters just aren't worth his time. Businesses tend to be the real hack targets. This applies equally to the exploding world of wireless networking.

"Accessing a wireless network requires technical savvy and specialized tools," notes Linksys spokesperson Diana Ying. "But people make the hacker's job easier by not enabling WEP encryption or implementing MAC address filtering, which acts as a VIP list to lock out all unauthorized users on a wireless network. WEP isn't perfect, but it is a good deterrent, like a car alarm. The majority of wireless networks today still remain completely open, without WEP, just waiting for a hacker to drive by."

/dev/null says recommended security steps for consumers generally aren't good enough. The hacker doesn't trust the abilities of antivirus companies to keep up with the latest threats. He advocates trusting common sense more than software.

"Good security requires diligence," says /dev/null, "but all security is a matter of acceptable risk. Decide what chance you're willing to take and tailor your security measures to suit it."

Make no mistake, hacking can be deadly serious for individuals and nations. Captured Al Queda computers indicated the terrorist organization was probing American public utilities and infrastructures, perhaps looking for weaknesses. Imagine if emergency water systems in Manhattan had been disabled Sept. 11, 2001. Perhaps white hats will be the firefighter-like heroes of possible future terrorist encounters.

It sounds like another Hollywood script, but the message about hacking is now positive. Hackers serve a valuable function, even black hats, because we can't afford to not take security seriously.

Most serious hackers want to help build a better, safer world. Ignore them at your own risk.

by William Van Winkle

(To read our "Is Encryption Safe?" sidebar and our entire interviews with Kelvin Wong and /dev/null, go to www.smartcomputing.com/cpumag/oct02/hackcover)