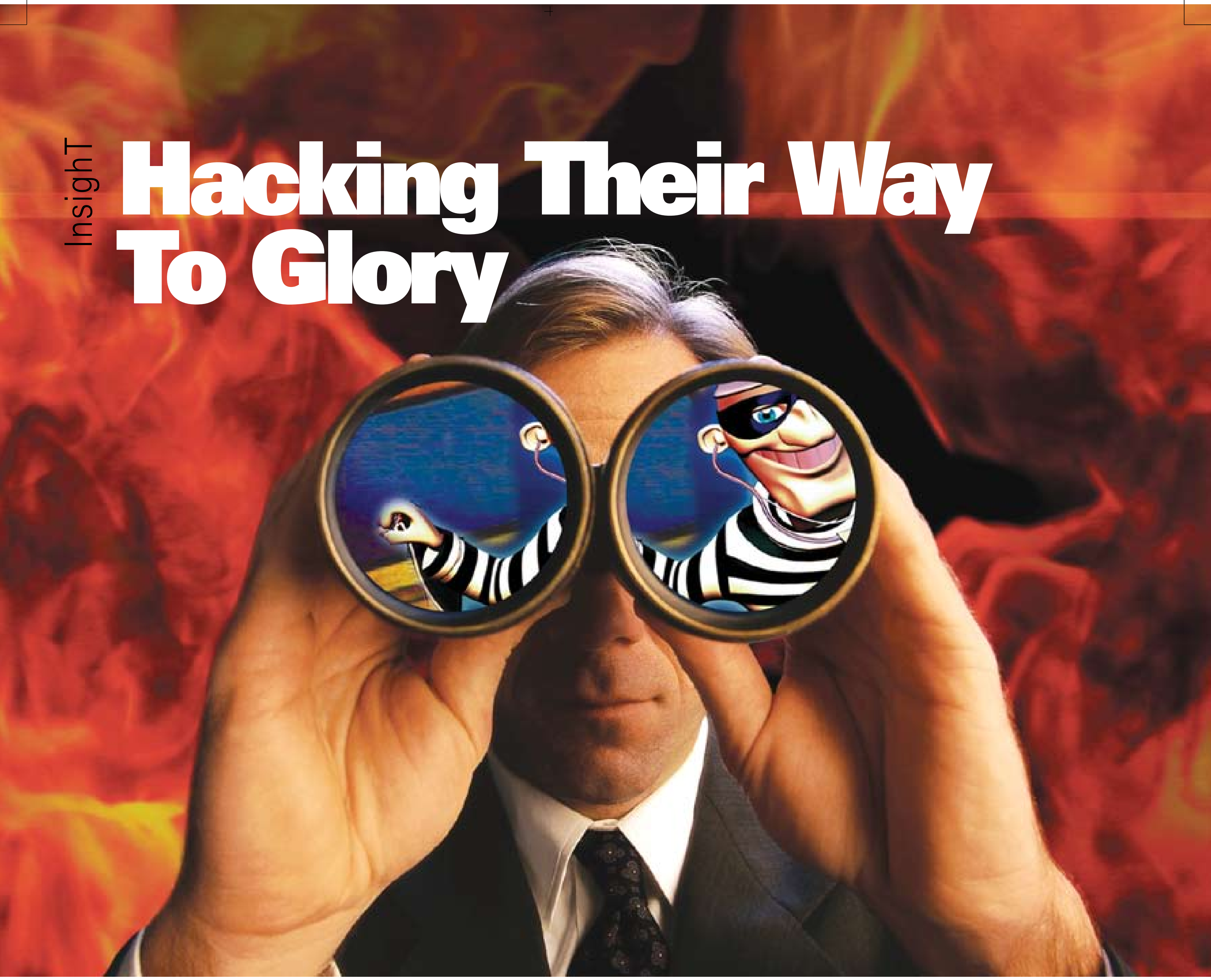
Hacking Their Way To Glory



In popular perception, hackers are criminals closeted in dingy rooms up to the wee hours of the morning, cunningly breaking into a bank's website to fill their own pockets. But like most popular perceptions, this one too is off the mark. We take a closer look at the world of hackers!

Charu Bahri
The author is a freelance writer and part-time LAN administrator at J Watumull Global Hospital & Research Centre, Mount Abu. She may be contacted at charubahri@gmail.com

If your website has been defaced and left you red-faced for failing to safeguard your company's online image, it is definitely time to rethink your security policy. There is no point in fuming or feeling embarrassed; just put your best foot forward, and get the right inputs to ensure the incident does not recur.

Of course, that is (like so many things) easier said than done. There are a number of experts lurking around, waiting to spot a loophole in websites and information systems. In fact, as websites gain in functionality and popularity, they become more vulnerable to unscrupulous persons who stand to profit even more by playing spoilsport. Fortunately, for every malicious hacker, there is also a good hacker willing to help you secure your website and other information systems.

Hacking: in black and white hats!

First things first—who is a hacker and how exactly do these two categories of hackers differ? Contrary to popular opinion, a hacker is an expert in every aspect of information systems—hardware and software. Sudhir Reddy, a senior software engineer with Yahoo!, or 'technical Yahoo!' as he describes himself, points out that, "Hacking is not confined to just software, it could even be hardware-related stuff. Basically, a good hacker understands systems in and out."

But there are experts and experts. While ethical (or 'true') hackers do not harbour any destructive intentions, 'crackers' are hackers who work their magic for malicious purposes. The difference between the two lies in their intent, not in their skills.

Arun Bansal, founder of HackingTruths, New Delhi, an institute offering courses in information security training, segregates hackers as white hats and black hats. White hats are hackers whom he says are, "Good guys who use their knowledge and expertise for good purposes. They do not cause harm to anyone. Black hats, however, are better known as crackers—these are guys with bad intentions. They perform illegal activities such as destroying data and stealing information."

Bansal likens the difference in the usage of their skills to the many uses of a gun—a tool used by the police as well as criminals—but with entirely different objectives!

Get them on board...

Since hackers are experts, they can contribute far more than just to a website's security.

Ahmedabad-based information security expert and a well-known hacker, Kalpesh Sharma, describes a hacker's level of expertise and usefulness in more precise terms. He says, "A professional can become a hacker only after working in every other sector—networking, programming, databases, hardware, software, encryption, etc. In other words, an expert can be a hacker, but a hacker cannot be an expert. Since hackers have a basic idea of the workings of every sector, they should be employed to foster growth and innovation in a programming set-up. A hacker's command over the various aspects of information technology is especially useful to add value to the challenging field of information security."

Bansal's take on the subject is that, "Hackers are highly skilled people who are not only jacks of all trades but also masters, as they are comfortable with many programming languages and are proficient in multiple operating systems like Windows, Linux, OS X, etc." Little wonder that he believes that white hats or hackers are people you are looking for to add to your team. Hackers are ideally suited to find new security vulnerabilities and (this is the big one) their solutions.

After all, hackers foster innovation—so why shouldn't we make the most of their skills? In Reddy's words, "A hacker has the passion to understand the internals of a system and make it work better for all." Or even, innovate and come up with a better method.

Reddy points out that hackers like Dennis Ritchie and Ken Thompson created the UNIX Operating System, which led to tremendous advances in the field of computers. Linus Torvalds created the open source Linux kernel—the core of the Linux operating system. And Richard Stallman calls himself a software freedom activist and has contributed lots of open source projects through the GNU Project.

Bansal agrees, saying, "Whatever the computer industry is today, is only because of hackers. Vinton Cerf known as the 'Father of the Internet'; Tim Berners-Lee, the inventor of the World Wide Web; Steve Jobs and Steve Wozniak who revolutionised personal computing by founding Apple; Bill Gates, the founder of Microsoft whose Windows operating system runs millions of PCs—all of them were hackers."

...if you can!

As Bansal says, "Hackers always try to find new ways to solve a problem. They always raise the bar and challenge themselves to perform better. They constantly address shortcomings and innovate. All this makes them well-positioned to add value to code. I consider them as a must in any programming team."

Evidently, hackers' skills may and should be harnessed to dramatically increase efficiency and foster innovation. However, this is not easy to do, as Bansal continues to present the challenge of including a hacker as

Hackers prefer open source software

According to 'technical Yahoo!' Sudhir Reddy, good hackers recommend using open source software, not just because it is better, but because it gives the user a lot of control. In his words, "You can tweak stuff as you want."

Further, Reddy points out that portals like sourceforge.net are contributing many open source projects to the community. People can join these and help build stuff that is useful to mankind. A good place for students to start working on their summer projects is http://code.google.com/soc/

part of a team. "Hackers hate doing repetitive work. But if they are given something they like, and which is suitably challenging, then they can be ten times more productive than a typical employee," he says.

The trick apparently lies in giving hackers something that they would like to do. But Eric Sink, founder of SourceGear, points out, "Hackers code for the love of coding. That's why they add value." Continuing in the same vein, he says, "You can't employ them to do anything useful unless your business happens to be doing what they want to do."

And that is a tad difficult, as every firm has its own agenda. So while you would ideally love to have a few great hackers on your team, essayist, programmer and programming language designer Paul Graham explains that it is not quite so simple. He cites a hacker's defining quality as the love to program. While "Ordinary programmers write code to pay the bills, great hackers think of it as something they do for fun, and they're delighted to find people will pay them for it."

So you may dream about a hacker specialised in computer security spending days and nights improving the quality of your product, and plugging its loopholes before these are exposed and cause extensive damage. But this will only happen if the hacker gets a kick, so to speak, from the work you lay out. Besides, as Paul Graham outlines, "Like all craftsmen, hackers like good tools. In fact, that's an understatement. Good hackers find it unbearable to use bad tools. They'll simply refuse to work on projects with the wrong infrastructure."

Understanding a hacker's mind

Hackers are basically more tuned to what they do, rather than the end result. Hackers are thus well positioned to add value to code, as they are more interested in the novelty of the process—the means, as opposed to the end. Sharma explains this as a hacker's love for taking up a challenge, to do something unique, something creative. In this regard, Reddy points out that a hack could be a quick-and-dirty patchwork or a carefully crafted program. It is just the cleverness that goes into the building and the usefulness of the work that matters.

However, Sharma believes that while the process is the primary aim, the solution (the end) cannot always be ignored. He says that while all hackers feel a thrill if they manage to penetrate a security system created by thousands of security professionals, some do realise that not all members of their clan have bona fide intentions. So they seek to plug loopholes before a disastrous situation occurs.

Reddy likens this process to hackers being a step ahead of crackers, applying their mental faculties to think of what the bad guys are up to and protect society from them. In fact, it is perhaps correct to say that it takes a hacker to crack down on a cracker. He points out how ex-cracker Kevin Mitnick—who now works as a security consultant for Fortune 500 companies—was nailed

"Hackers always try to find new ways to solve a problem ...They constantly address shortcomings and innovate... I consider them a must in any programming team."

—**Arun Bansal**, founder of HackingTruths, an institute offering courses in information security training

Identifying hacker potential

What are the qualities of a good hacker, or would-be hacker, that would serve an information security or penetration testing team in good stead? For, given the legal provisions that the Information Technology Act 2000 lays out—that hacking is a technical crime irrespective of whether the criminal was known as a hacker, ethical hacker, cracker or information security expert—a continuous penetration, testing and improvement of information security systems is only possible if the expertise is available in-house, in which position it may be protected from legal action.

Information security expert Kalpesh Sharma emphasises that hackers working in the security field must have a background of extensive research and study, and preferably hold reputed certifications like CISSP, MCSE, etc, and not merely be strong on computer fundamentals, networking or programming. Hackers should ideally also be well-versed in cyber law.

As far as hacking skills are concerned, a hacker should be able to work through 128-bit encryption, which is nowadays accepted as a security standard in financial transactions.

Hacking, live on TV

During a live session on IndiaTV, with several luminaries (including the IT minister, the director of Indiabulls Securities, and technical and legal experts online or in the studio), Kalpesh Sharma proved that many of India's Internet banking, shopping and trading websites are vulnerable to hackers.

Sharma's intention was to alert India's population and, particularly, heads of information security departments, of the loopholes that need to be plugged. Interestingly, one of Sharma's feats was to hack into the Indiabulls' trading website, and then transfer money from his wife's account to his bank account. His wife's account was chosen to protect the channel, and Sharma, from possible legal action.

According to IndiaTV, Gagan Banga, Indiabulls' director who was online, refused to acknowledge Sharma's achievement and claimed that the transaction hadn't taken place at the backend, implying that the money transfer cheque would not be issued. However, the next day, IndiaTV showed its viewers the cheque that had actually been issued, thus proving the loophole in the website. Equally revealing is the fact that when the same hacking moves were performed the subsequent day, they did not work—implying that the error had been corrected overnight!

by hacker Tsutomu Shimomura, in a process well described in Shimomura's book *The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It* or the movie *Takedown.*

Think like a hacker

It would be immensely useful to involve hackers in your team. But if Reddy's opinion is correct—that all it takes to be a good hacker is a passion to know the 'why, what and how' about things around you— then you could possibly encourage your IT staff to develop hacker-like thought processes to evolve into more effective team players.

At Yahoo!, for instance, hack days, or day-long events are organised during which engineers are encouraged to take a day off their current projects and work on building something 'cool.' Most of these 'cool' projects go live on Yahoo! for public use. In fact, Yahoo! and other like-minded companies have now opened the participation of the general public in such hack contests [see links of interest].

The best overall hack, or innovation, to come up in 2006 was titled *Blogging in motion*, and constituted the creation of wearable technology enabling one to blog from a purse. The winning team included Diana Eng, Emily Albinski and Audrey Roy. They used two Yahoo! APIs—ZoneTag, Flickr—and some third party APIs—a sewing machine, a soldering iron, a Nokia 6682 schematic and a pedometer! For more details of their feat, visit http://www.blackboxnation.com/bim/blogginginmotionpurse.html

Dare you invite a hacker to your table?

For all we know, there are budding hackers all around us—crying out for a chance to prove themselves and make meaningful contributions to society. Perhaps, information technology companies should reach out to more would-be hackers, and encourage them to work on security enhancing projects. Which brings up another pertinent point—are companies sufficiently open-minded to invite hackers to be a part of their team?

Sharma believes that while hackers have made a lot of contributions on an international level, in India, no one cares. "A hacker's true value is in the USA, UK and in the Middle East. Even Pakistan contributes more towards the security field. Although so many vulnerabilities exist in the security of MNC Web applications in India, our government is still sleeping," he quips.

Given the talent at the disposal of hackers, commercial establishments like airlines, 5-star hotels, travel and insurance companies, etc, should be seeking their services to identify and rectify any risks associated with using their websites. Information technology companies, too, should use hackers to improve the quality of their security products.

All said and done, hacking isn't bad—cracking is! It is about time we changed our mindsets and brought on board a few brilliant minds in order to hack our way to success. I.T.

Paul Graham, essayist, programmer and programming language designer

> "Good hackers find it unbearable to use bad tools. They'll simply refuse to work on projects with the wrong infrastructure."

TitBits

Save water, Save Planet Earth!

On the occasion of the Earth Day, Intel India and the World Wildlife Fund India (WWF) organised an essay-writing contest, based on the theme of water conservation. The endeavour was aimed at spreading a word about conserving water and also at making the youth aware of their responsibility to save the environment and conserve the natural resources. Six hundred schools from six major cities of the nation participated in the event. "With water resources fast depleting, spreading awareness about conserving water is the need of the hour," said Frank Jones, president, Intel India. Out of the 900 participants, attractive prizes were given to the eight national winners. The two top winners received laptops, the next two were given iPods and four others received consolation prizes.