The Washington Post

INTO THE BREACH

By Pamela Ferdin
April 4, 1998

In a chaotic room crammed with computer terminals and circuit boards, a long-haired man in black jeans -- "Mudge" by his Internet handle -- fiddles with the knobs of a squawking radio receiver eavesdropping on the beeps and tones of data transmissions.

Nearby, a baby-faced 22-year-old in a baggy sweat shirt, nicknamed "Kingpin," analyzes reams of coded equations to break password sequences percolating on his computer screen. Other figures with equally cryptic identities toil in an adjoining chamber, their concentrated faces lit only by a monitor's glare and the flicker of silent television sets.

This is the L0pht, pronounced "loft," a techie operations center in a suburban warehouse several miles from city center that is inhabited by a group whose members have been called rock stars of the nation's computer-hacking elite.

The seven members of this computer fraternity-cum-high tech clubhouse have defeated some of the world's toughest computer and telecommunications programs and created security software that is the gold standard of corporate and hacking worlds. By day, they are professional computer experts, mostly in their twenties and thirties, with jobs and even wives. By night, they retreat to the warehouse and their electronic aliases troll the Internet for security gaps.

Hacking mostly for the challenge, they have exposed security flaws in Microsoft Corp.'s leading network operating system, revealed holes in Lotus software and figured out how to decode pager messages and mobile police terminal data, among other feats.

Hackers typically get into supposedly secure computer systems and pinpoint security breaches by deciphering elaborate number, letter and symbol combinations designed by manufacturers to protect their products. If security is breached, users risk having everything from private e-mail read to databases erased.

A single, unintentional hack is not illegal, the U.S. attorney general's office here says. But repeat intruders face criminal penalties, especially when they compromise and damage confidential government, military or financial information.

The risk of such intrusions was highlighted recently by an Israeli teenager known as "the Analyzer" who broke into unclassified Pentagon files and recruited several U.S.-based proteges into his game. Nobody has been charged in that series of pranks, but U.S. defense officials took it seriously at the time.

L0pht members pride themselves on a less invasive and more altruistic goal just this side of the law: To locate and document Internet security gaps for free for the sake of consumers who have been led to believe their online transactions are secure.

"We think of our Net presence as a consumer watchdog group crossed with public television," said "Mudge," a professional cryptographer by day who declined to identify himself for security reasons. "At

this point, we're so high profile . . . it would be ludicrous for us to do anything wrong."

Even companies whose products have been hacked for security weaknesses laud the social ethos and technical prowess of the members of the L0pht, who frequently notify manufacturers and recommend fixes before going public with their finds. Unlike villainous hackers labeled "black hats," who probe cyberspace for profit and malice, Robin Hood-style "white hats" like the L0pht are generally accorded respect, and even gratitude.

"They forced us, well, encouraged us, to be diligent about providing information to our customers about how to protect their environment," said Michael Simpson, marketing director for Novell Inc., a prominent network software provider. "You won't stop hackers doing what they do. The best thing is to use their information to your benefit to make your own product stronger."

L0pht members formally banded together in 1992 to acquire a lease, but they began more than a decade ago as a loose association of friends driven by their obsession. Several became acquainted over the Internet years before they met in person; others grew up together as brilliant adolescent misfits who hacked into phone lines and disassembled household appliances.

These days, they retrieve equipment from flea markets and dumpsters, rebuilding systems so they can simulate security break-ins. When a hack is successful, they post an advisory on their Web site (www.l0pht.com) alerting consumers to a software or operating system vulnerability and providing the equivalent of a hacking recipe to demonstrate their point. Then they move on to the next challenge.

Their work has paid off with L0pht security formulas becoming standard tools for hackers and corporations. A limited number were sold via CD to cover rent and utility bills. "Space Rogue," for instance, a single 30-year-old Macintosh guru with a cellular phone dangling from his belt, compiled a popular collection of hacking tools entitled "Whacked Mac Archives." "Kingpin," a hardware virtuoso arrested at age 16 for breaking into systems considered sensitive by federal authorities, designed a telephone fraud detection system and pager decoder.

One member's wife compares the L0pht to a rock band, and the clandestine clubhouse is part "Animal House," part NASA. Computers and arcane technical manuals are surrounded by a generous supply of empty Ipswich Ale bottles, Chinese takeout menus, ratty couches and misshapen mannequins hanging from walls. But Delta Upsilon would be hard-pressed to rig a similar Web browser to its toilet, for use instead of magazine reading, or arrange interviews with Jim Lehrer and the BBC.

The group has also earned the respect of its purported targets: firms such as Microsoft that increasingly rely on hacker know-how.

In the L0pht's most widely publicized hack, "Mudge" and a colleague assaulted Microsoft's Windows NT operating system last year and found inherent flaws in the algorithm and method designed to hide user passwords. They demonstrated the security breach by posting their victorious code on the Internet and

showing how it was possible to steal an entire registry of passwords in roughly 26 hours, a task Microsoft reportedly claimed would take 5,000 years.

"It's big. It's bad. It cuts through NT passwords like a diamond tipped, steel blade," boasts advertising for the latest version of their security-auditing tool, dubbed "L0phtcrack." "It ferrets them out from the registry, from repair disks, and by sniffing the net like an anteater on dexadrene."

Microsoft took notice and, in an unprecedented move, executives invited the L0pht to dinner at a Las Vegas hacker convention last year. They have worked with the L0pht to plug subsequent security loopholes while simultaneously adding hacker-style techniques to in-house testing.

"It's like a challenge for them, which is great for us too," said Karan Khanna, a senior security product manager who attended the dinner.

No one knows how many hackers operate out of Boston, the Silicon Valley of the East. But the FBI, which launched a computer intrusion squad here last year, estimates that up to 18 intrusion complaints are under investigation locally at any one time. Few are traced to hackers, and none has involved the L0pht.

That is as it should be, some say. "If Windows magazine assigned a writer to crack the security of {Windows} NT, everyone would say it is perfectly acceptable for consumers to be better informed," said Mike Godwin, a lawyer for the Electronic Frontier Foundation. "The only difference is these guys aren't publishing a magazine, they are publishing on the World Wide Web."

In doing so, the L0pht is grabbing the world's attention. But for all their skill in unscrambling the great riddles of technology, they remain baffled by some fundamental mysteries of life. Asked what puzzle they would most like to solve, "Kingpin" replied: "Girls." CAPTION: The L0pht in Boston, where they hack. Standing, from left, are Brian Oblivion, Kingpin, Space Rogue, their associate Meg A. Haquer and Weld Pond. Seated are, from left, Stefan Von Nuemann, left, Mudge and Tan.