COLUMBIA SUMMER SPECTATOR

May 23, 1984

VOL. CVIV—No. 1 NEW YORK, NEW YORK

© Columbia Spectator Publishing Company

Sovern calls for peace

By THOMAS VINCIGUERRA

Unseasonably cool temperatures and occasional drizzle threatened last Wednesday's commencement exercises but did not put a damper on the enthusiasm of Columbia's 7,497 latest graduates; the "magnificent graduating students of 1984," as President Sovern called them, made a smooth move into the real world with many cheers.

For the first time since the announcement of coeducation in January, 1982, Columbia College conferred degrees on women—six transfer students from the School of Engineering and Applied Sciences.

In the graduation address, traditionally given by the university's president, Sovern called upon the graduates to "help to determine the strength of our society and the effectiveness with which we conduct ourselves justly in the world" by attempting to find alternatives to war, which he called "a habit we cannot seem to break."

Sovern expressed concern over interna-

See GRAD, 3►

SPECTATOR/ED KEATING

PEACE: The thrust of President Sovern's commencement address was peace and a reduction of world tensions. "War has become a habit we cannot seem to break," he said, quoting John Lennon's line, "War is over—if you want."

State approves $500 million hospital plan

Presbyterian may build on Baker Field

By ANNE KORNHAUSER

State approval of Presbyterian Hospital's $500 million revitalization and construction plan last week increases the likelihood that the university's Baker Field will become a construction site for a new community hospital, Provost Robert Goldberger said Monday.

Thus far, the university and the Hospital have reached only an "'agreement in principal" which allows the Hospital to use a certain portion of Baker Field, located at West 218th Street, for the construction of a new community hospital. But Goldberger said the state's authorization of Presbyterian's preliminary plans makes a formal contract between the two parties more likely. "Now that they have their certificate of need, they're going to want to have an actual agreement," Goldberger said.

Columbia has agreed informally to sell five acres of Baker land to Presbyterian so the Hospital could build a 300-bed, $100 million community hospital there. In exchange, the university has said it would receive about $5 million and an additional one and a half acres of land across Broadway, which Columbia plans to use for football practice fields to replace those that would be lost to the hospital.

The state approved a five-part program, including the three-story community hospital, and the revitalization of Presbyterian's teaching hospital at the Columbia-Presbyterian Medical Center, which is jointly administered by the hospital and the university and is located at West 168th Street and Broadway. This will involve the construction of a new building at the Center to provide an additional 750 adult beds, according to Richard Zucker, the hospital's director of public interest.

According to Zucker, construction at the Medical Center would begin later this year and continue through 1989. But before the hospital can start building, the state must grant a second approval, this time of the hospital's architectural plans, which Zucker said he expected would be submitted

See HOSPITAL, 3►

BC: Women stand tall in the '80s

By ANNE KORNHAUSER

Speeches boasting of a new role for the educated woman in the 1980s highlighted Barnard's 92nd commencement ceremonies last Wednesday.

Ellen Futter, Barnard's president, and Vartan Gregorian, president of the New York Public Library, spoke of the unique experience of a women's education and of the wealth of opportunities that a technologically advanced world offers an intelligent and active Barnard graduate.

Both warned that the students' primary responsibility is a contintuing commitment to "learning to learn." Futter, addressing the first class to spend all four years under her admnistration, added that "as young women going forth in the Orwellian Spring of 1984, you have more oportunities available to you than any young women ever."

The seniors sat eagerly through two hours of speeches and awards before hearing their names called by Barbara Schmitter, vice president for student affairs. They then waited another three hours before formally having their degrees conferred at the university's commencement on Low Plaza.

Earlier, at Barnard's Lehman lawn, Futter had lauded the Barnard-Columbia coeducation agreement under which Columbia College admitted women for the first time this year and Barnard remained a single-sex institution. "You came to Barnard at an enormously exciting and important time in her history," Futter said to the graduates. "You have witnessed and participated in the beginning of a new and far more harmonious era in Barnard-Columbia relations.

"You have seen the re-affirmation not only of our relationship with the university, but also of our role as an independent college for women with its own outstanding faculty," Futter continued.

Overall, the ceremony was quieter than last year's, which had centered around a controversy over giving Barnard's Medal of Distinction to U.S. Ambassador to the United Nations, Jeanne Kirkpatrick. This year's class was also considerably smaller than the 675 graduates of the Class of 1983, with only 550 students receiving degrees.

Gregorian, who received a warm welcome at the ceremony, emphasized in a 45 minute speech the merits of a liberal arts education in a world which he described as

See BARNARD, 3►

SPECTATOR/ED KEATING

HEY, BUDDY, IS THIS HELL'S KITCHEN? Festivities, fun, and a lot of food were jammed into about twenty blocks at the 11th annual Ninth Avenue International Festival this weekend. But over a dozen versions of the "perfect" Pina Colada stole the show on this sunny Saturday afternoon.

TC cafeteria fined by city Health Dept.

By PHILIPPE ADLER

The Department of Health may close Teachers College Cafeteria if a final inspection by them, anticipated for Tuesday, shows that mice and insects are still present in the grounds.

Nicholas Titakis, acting director of the New York City Department of Health's Administrative Tribunal, said two inspections in the last two months turned up persistent problems "with active insects and some evidence of mouse droppings," for which the school was fined $745. These were the only two serious, or "Class A," problems found by inspectors, Titakis said.

The cafeteria was on a list of 49 eating establishments cited by the health department for violating the health code. The list was published in the Sunday newspapers.

Bettye Caldwell, manager of the cafeteria, refused to comment. Victor Mainente, Controller of Teachers College, said "I don't think we'll have any problems" passing a final inspection by the Department of Health because "we've been after the exterminator's company now, on the basis of these inspections, to do a more effective job."

The final inspection, said Mainente, "is rumored for next week, May 29th." By law the Department of Health must give 48 hours notice of a final inspection, Titakis explained. Mainente said "it's supposed to be sort of a surprise." He said that he and the school's Buildings and Grounds manager were "constantly after" the exterminators and that on May 12 the cafeteria had been "bombed" for insects.

The violations were discovered on March 27, during an initial,

See CLASS A, 3►

Attack of the hackers

Computer break-ins: they're coming for you

By BOB SABIN

We may be in trouble.

The hackers are coming: high-tech hoodlums operating in an electronic underworld. Last summer they broke into computers at the Los Alamos nuclear lab and at Sloan-Kettering Cancer Center. Tomorrow, they might have your tax records.

Not that they'd want them, though; for most of these teenage enthusiasts—who operate from their home computers with a device that lets them communicate over the phone lines—the thrill of making the connection is reward enough. But as more people find themselves with the equipment and know-how to explore the vast river of valuable information that pulses through our electronic society, the odds increase. It may be only a matter of time before criminal incentives seep into the world of microcomputing and make hacking a lucrative business.

There is no way to completely eliminate this sort of activity, although a crash course for the general public in personal computing ethics might help. Even then, large sums of money will still need to be spent on protection, and much legislation passed, before anyone is likely to feel safe again. Somehow, no one ever envisioned that the coming of the computer age would result in gangs of schoolkids attempting to prove their mettle by punching their way into the grown-up's machines.

Computer break-ins have been going on for almost as long as there have been computers, particularly on college campuses where students learn the specifics of computing on larger systems that are shared by many terminals throughout the school's computer centers. On these computers, the "operating system," a permanent program designed to handle housekeeping chores (such as keeping one's user programs filed separately from someone else's) is a prime target for bored hackers looking for a challenge and the thrill of voyaging into forbidden territory. By either fooling or altering the operating system, the hacker can penetrate the computer's built-in security. The computer, mistaking the hacker for someone else, perhaps the system repairman, will grant him special privileges and allow him access to more of the information in the data banks. For a college student hacking on his university's machine, this can mean getting into another student's projects, or stealing the computer time another student has been granted. At worst, the mischief can go as far as "crashing" the system, bringing it to a complete halt.

These "time-sharing" computers are of the same type as those used by industry and a number of government agencies, including the IRS and the Defense Department. In many cases, the wide-ranging geographical interests of these institutions require them to make their data available to all of their branches, and this is where a "modem" comes in. An acronym for "modulator/demodulator," modem is a device that takes a computer's digital information and translates it into a series of pulses that can be transmitted over a standard telephone line, somewhat akin to speech. Another modem connected to the line can then convert the information back into the sort of material that can be interpreted by the communicating computer or terminal.

To cut telephone costs, a company or agency might connect their machine to the lines through a huge data transfer network that services many customers' computers at once. These networks, like the one operated by GTE Telenet, save money by using pauses in the data transmission of one computer to send another computer's data over the line to a different destination. In this way, the line is used at maximum efficiency; waste that normally occurs on a single phone line is eliminated. The many different routings betwen computers and user terminals are achieved through entry codes that tell the data network which computer the user is addressing; these codes are punched in after a local phone connection is made to the network.

It was Telenet's line that seventeen-year-old Neal Patrick and others in his Milwaukee-based computer group penetrated last August. After tinkering around (harmlessly in this case) in a low-security computer at Los Alamos and in the Sloan-Kettering machine (where an attempt was made to fool the operating system into storing other users' passwords for later retrieval by the hackers), they were detected and traced by the FBI. As quickly as the agents at the door could say, "Your little monster is in trouble," Patrick's parents had hired a lawyer for him who secured immunity from prosecution. Patrick has since gone state's witness for a government investigating committee, which must have sat there agog that such a nice kid could be involved in such surreptitious activity. Concerned for his fellow hackers still vulnerable to indictment, Patrick responded to his immense publicity by offering his version of "The Patrick Neal Story" to anyone interested for the mere sum of $20,000, which he said he would then donate to the rest of the group for legal fees. Happily for us, it appears there have been no takers, nor has there been any further prosecution by the FBI.

Important here is the theme that ran through all of Patrick's testimony. He and others in the group who were quoted anonymously in the prints repeatedly emphasized how easy it was to get into these systems and how much damage they could have done if they'd had malicious intent. Patrick cited the lax security of the Los Alamos system for a House Investigative Committee thus: "If they had just changed their password, we couldn't have broken in."

Other cases of hacking around the country have resulted in financial damages for institutions whose computers have been taken down or whose data has been altered or deleted. In one reported case, a computer service in Kentucky that provides race and breeding statistics for every thoroughbred in the country was penetrated by a hacker who cost the compnay over $100,000 in lost revenues while they took their regular customers off-line to facilitate an FBI tracing scheme. In another instance, a San Francisco leasing firm lost $260,000 when someone broke into their system and filled the files with obscenities. And in a civil suit filed by Columbia, the College charged that a hacker who had sought to crash one of their computers had cost the school thousands of dollars.

All of this may seem like relatively harmless prankstering that costs a few wealthy organizations some pocket change to straighten out their systems and change their security passwords, but our increasing reliance on computers in all facets of society makes the potential threat to human life tremendous. In the Sloan-Kettering break-in, the hackers unknowingly modified patient files controlling radiation treatments. A 1979 Air New Zealand jetliner crash that killed 257 people was found to have been caused by the altering of the jet's computerized flight plan without the pilot's knowledge. The New York Times reported that in November 1979 and June 1980, national defense computers "erroneoulsy reported that the United States was under attack, and the armed forces were put on alert."

The message is clear: it doesn't take much. Our world is rapidly going digital, and one small computer error—brought on by tampering, equipment malfunction, or a simple human mistake—can go a long way.

I wanted to learn more about hacking, so I contacted Gerald Leitner, who teaches a course here in the design of operating systems. If the operating system is at the core of this game—the electronic personality in every machine that waits to be conquered—it seemed plausible that someone with an intimate knowledge of this kind of program could tell me something about the vulnerability of these systems.

But Dr. Leitner was uncooperative from the start, and when I politely persisted, he became suspicious. After stating that he knew nothing about hacking and what steps an intruder might take to worm his way into these computers, he grew increasingly nervous, and finally implicity accused me of a deeper, clandestine motive in questioning him. "Even if I knew," he exclaimed, "I wouldn't tell you."

It was obvious that I wouldn't get anywhere by going through established channels. So I decided to bypass them, and go right to the hackers—plug directly into the network, as it were.

This the first of two articles on computer break-ins. Next week, the author delves into the dark world of the hackers and sheds some light on their shadowy activities.

Features

Attack of the hackers

Part two: A cook's tour of computer crime

Note: This is the second of two articles on computer break-ins.

By BOB SABIN

A survey of the university's many terminal rooms eventually found me at the bottom of a dank, isolated stairwell in the bowels of the Computer Center on the west side of Uris. This was SSIO, Self Service Input-Output, a meeting and work place for the College's computer students. Opening the door, I half-expected a stereotype: a batallion of horn-rimmed Poindexters staring through thick lenses at green phosphorous screens, their socially crippled brains whirring audibly, drowning out the clacking of the printers.

I was relieved to find a varied crowd intently working at the terminals, but surprised, upon entering the small connecting office, to find at least one student who was somewhat different from the rest. Perry Metzger is a full-time computer science major in the College; he's articulate, a bit precocious, and just barely five feet tall. That might be unusually short, except that Perry Metzger hasn't yet seen the far side of a growth spurt. He is only 15 years old.

After discovering computing on the Digital Equipment Corporation PDP 8 minicomputer owned by his old high school, he quickly advanced to where he is now three years ahead of his ex-classmates. He appears at ease in his new peer group and spends part of his time in the System Consultant's office, just chatting about these beastly devices with the operator on duty and assisting other students who are having difficulties on the university's time-sharing DEC 20. ("I'm sorry if I talk a lot in computerese," he apologized right off. "I tend to do that when I'm discussing computers.")

The day I visited SSIO he was in the office with Eric Hochman, another computer student who serves as a watchdog and general overseer of the system.

"Around here we have pretty good security," Hochman told me, responding to a question about student break-ins at Columbia. "Everything's on back-up tapes—it's hard for someone to do damage that can't be repaired, even if they do get it. It does waste time, though. It's a criminal nuisance—we're not amused by it."

Not amused? Apparently not. Cases of student tampering are handed over to the dean and may end in criminal or civil prosecution, as it did for one hacker who was caught stealing computer time:

"The last person who tried this was taken away by the police," Hochman said. "He got his hands on an account and managed to replace the exec [a part of the operating system] so that he didn't have to log in to use the computer. One fine day he was sitting in one of the terminal rooms, mounting tapes without being logged on and doing strange things, and someone noticed. He was basically carried out."

"Break-ins are a real problem on commercial networks like Telenet," Metzger said. "The trouble is compounded by all these bulletin board systems where anyone who wants to hack can probably find out anything they need."

I'd heard about the bulletin boards. These were message services, usually microcomputers and modems, privately owned, that anyone with his own computer and a modem could dial up to send and receive electronic mail. There were literally hundreds all over the country, Metzger told me, and many were used by hackers and software pirates as a way of trading tips and publicizing computer telephone numbers and passwords. Pirates are computer buffs who make a hobby of breaking the copy protection codes installed on copyrighted software. When I asked for some phone numbers, Hochman punched up a program on his terminal. A printer located just outside the room began spewing a list.

Metzger jumped up to tend to it, and after a few moments, popped his head in the doorway. "It's a mile long!" he said excitedly, and I got up and followed him out. The printer was churning away. There was already three feet of copy. Three or four minutes later it finally stopped, but not before it had read out nine feet of numbers. At 75 bulletin boards to the foot, that's 675 systems tied up strictly for communications among computer enthusiasts. They originated from area codes all over the country. Some looked pretty legitimate, but others had names like "Pirate's Cove." I wondered aloud how anyone could afford to call bulletin boards on the other side of the continent, much less dial up a computer and spend hours hacking at it.

"There's something that hackers call 'phone freaking,' " Metzger explained. "They will steal someone's MCI or Sprint number and use it so they can break in around the country or call up bulletin boards without paying for the telephone charges."

But how do you get someone else's Sprint number?

"With an autodial modem it's simplicity itself," Metzger said. "If you know the local Sprint or MCI access number, you have the modem call repeatedly and tap out various combinations of numbers until, finally, it gets one that works. The autodial modem takes very little time to find one, because the dialing is very fast.

"MCI is cracking down on this sort of thing now," he continued. "If they suspect that someone's number is being used they'll check up on the person and get the line traced. It's a federal offense; they can get that done. So now the hackers do other things—for instance, recursive dialing of MCI. You call up MCI, find a number. Then use the MCI number and call up, say, Sprint, and get a number there, and loop it through a few times—to make it more difficult to trace."

I grew curious about actual break-in procedures. "People like the Four-One-Fours [the Milwaukee-based group that broke into the Telenet system last August] got into the newspapers, but they're not really the problem," Metzger said. "The reason people can break into systems so easily is because they *make* it so easy. There was one system, for instance, where at the screen prompt, when they had been attempting to log on, they typed in HELP PASSWORD and it gave them a default password. I mean, when you have security like *that*. . ."

The question of computer security brings up the issue of "user friendliness." User friendliness refers to how accessible a computer owner or manufacturer wants to make the computer's functions and data to a new or less sophisticated operator. A user friendly system, for instance, might have an operating system that will help a user learn about the computer by offering a menu of commands and explaining them. A computer that offers a password upon request might jokingly be called *very* user friendly, and security on such a system will be accordingly lax.

"You do what you feel like doing—you **explore** . . . if you get high enough privileges, you can get into documents you're not supposed to read, or crash the system."
—Perry Metzger

To demonstrate, Hochman dialed up a computer at Carnegie-Mellon Univeristy in Pittsburgh, using the keyboard at his desk. "I don't have an account there," he said, but without any passwords or ID codes, we were able to connect in. The Carnegie computer responded with a message identifying itself, then the screen cursor spit out the "at" symbol (@), and just waited. All we had at that point was the telephone number for the access line. That might have been available on any bulletin board.

"Okay," said Hochman, "I'm not logged in, I'm just there. Now, I might try this. . ." He typed in one character that any hacker might punch if he were looking for help: a question mark, followed by the return key. The screen immediately filled with words—a listing of user commands, with a short blurb for each one. "Most of these things you can't do without being logged in," he said, but then he typed in WHERE, one of the commands noted, and the computer came back with a list of those people who were presently on the system, along with their ID numbers. "Now I know what the ID numbers look like," explained Hochman. "They tend to be two letters and two numbers."

He stopped short of actually trying to enter the system, but Metzger went on to explain the procedure. "Now you can type in a guessed ID," he said, "because they're all four characters, and try something like LOG IN to get on. Then you guess at passwords. On some systems there are default passwords, so you try things like TEST or REPAIR, or, if it's a school's computer, STUDENT, or even GUEST."

Let's say you've gone through all the guessing and get logged onto the system. Then what?

"You do what you feel like doing—you *explore*," said Metzger. "If you happen to find an account with privileges, you are permitted to make modifications to the operating system or execute certain programs that the general user doesn't have access to. If you get high enough privileges, you can get into documents you're not supposed to read, or crash the system. If you *don't* get privileges, you're a plebian, and you'll just explore the system and come try again.

"Hackers generally get into benign mischief, like reading things," he said, "but occasionally, they accidentally destroy things."

• • •

The hackers have not won their secret war yet, and steps are being taken to make sure that they never do. For example, organizations that must keep their computers connected to the telephone are almost universally tightening security, and new legislation is being presented to ensure that break-ins can be treated with harsher punishments.

But how do the hackers feel about it?

"Most of them don't view it as a crime," Metzger said, adding that he knows a number of computer hobbyists who hack as a passtime. "Usually, they're not there to make trouble. It's sort of like climbing Mount Evereste—the thrill of getting in is the most important part. And, also, being able to laugh about the stupidity of the security on most of the systems. It *is* a

Both Hochman and Metzger agree that such illicit use of computers is giving the computer enthusiast, and the term "hacking," a bad name.

"Hackers, in the sense of people who break into systems, are a minority," Hochman observed. "Most people who know about computers and work on them re not trying to break into anything. The strict definition of "hacker" is anybody who likes to work on computers and likes to learn more about them, but the word is picking up a bad reputation because of a small number of people who very loudly say they are hackers and are trying to break into things."

"You should not think of them as being hackers in general," Metzger advised. "Look, I like to sit on the system, play around with it, read mail messages and new documentation files—I consider myself a hacker. But the guy who logs on to Telenet, hops across a couple of satellite connections, and breaks into Los Alamos, is a person with a slightly warped sense of, shall we say. . ."

Metzger stopped short of making a judgment and hesitated a moment, to reconsider.

"Well," he went on, "I could easily see myself doing that—if I did not think it was wrong."

"So the only thing that separates you from them is that you have some ethics?" I suggested.

"Yes," he quickly agreed, adding, "but I also have some fear, because I know that they'll catch me."