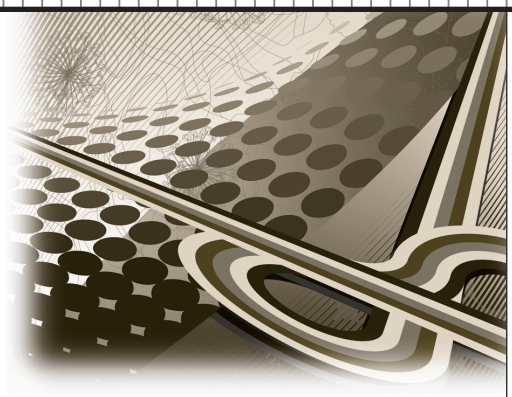
Honor Among Thieves



David Alan Grier, *George Washington University*

Without a human organization that can sift information and raise the gold from the dust, knowledge will die as rumor and innuendo will overwhelm any truth that may be making the rounds.

For years, I have refused to acknowledge that undergraduates are worthy of first names. First names suggest an intimacy with the adult world that these senior adolescents have not yet earned. They have not demonstrated the qualities that entitle them to a place in the community of educated men and women and so they deserve only the formal appellation of their family. Almstead. Dumbacher. Hooper. Eilts. Garlinghouse. Rasche. Only when they have accomplished something in their own right are they entitled to their own name.

"Major X" is one of the few students who has earned an exception to my general rule about names. Shortly after receiving her commission—she is an officer in the US Army—she joined an elite cybersecurity team. In this role, she is supposed to protect her identity, and so decided that I could not refer to her by either her family name or her personal name. Major X she became, at least to me.

KEEPING IN TOUCH

Over the years, Major X has helped me to understand the changing nature of cybersecurity. She has usually been quite responsive to my requests for information. Within a couple hours of receiving an e-mail message, she'll give me a call, chat a bit about her current assignment, answer my question, and ask about friends from her graduating class.

However, last summer, Major X vanished for a couple of months. As August changed to September, she sent me a quick note to say that she would call in a week. "On a job," she wrote. "Can't talk. Look at my photos on Facebook."

Major X is an inveterate photographer, though her pictures tend to be group shots of friends rather than images that tell a story. Over the past years, she has posted pictures of a beach volleyball game on some tropical island, a shopping spree in Harajuku, a day at one of the Disney theme parks, and an evening at the Grand Théâtre de Genève in which she is wearing a designer gown that has nothing in common with the clothes she favored as a student.

As I paged through the most recent set of photos, I resurrected a worrisome doubt that had haunted me for the past year or so. Did these photos represent real activities, I wondered, or did she post them to establish a false identity? After all, she has a career in computer intelligence and holds a high-level security clearance. Also, she is a cautious and reserved person. I have watched her move through a dinner party and leave no trail that suggested the nature of her job or the name of her employer. She has few reasons to expose her private life to the public or to suggest to outsiders how she thinks, how she strategizes, or even how she organizes her free time.

When she finally called, I was curious to hear the story of her summer. "So, X," I asked, "how have you been?"

"Fine," she said, clearly giggling at my question. "I have been very fine."

As X normally appends the word "sir" to almost anything she says, I decided to press a little harder. "What have you been doing this summer?"

At this point, the giggle became an open laugh. "You'll never guess," she said. "I gave a talk at DEF CON."

For a moment, I was at a loss for words. After all, DEF CON is not only the largest and most notorious of the computer hacker conventions, it is also held in the Nevada desert in the heat of summer. X would have gotten no stronger response from me if she had said that she just returned from a poker tournament hosted by the North Korean Secret Service.

DEF CON?" I asked.

 Published by the IEEE Computer Society 0018-9162/09/$26.00 © 2009 IEEE

"Yes," she replied.

And you were a presenter?" I continued.

"Yes," she said.

"And did they know that you were in the military?"

"Of course," X added.

"They didn't care that you weren't a hacker?" I tried.

"How do you know that I'm not?"

This last question was accompanied by another unsuppressed giggle, a giggle almost unbecoming to an officer. I believed that I knew the answer to the question, at least knew it as well as anyone could. After all, I had known Major X when she was merely sophomore X and was struggling through the lessons of algorithms and data structures. Yet, I had to admit that I probably harbor doubts about anyone connected to the hacker community just as we generally have doubts about anyone whose accomplishments are shielded by the public face of an organization.

AN UNCONVENTIONAL CONVENTION

At base, DEF CON is a conventional organization, a trade show and nothing more. It has talks, exhibits, breakout sessions, and social events. The attendees pay a hefty fee, wear a badge, and are given the opportunity to take a room from a special block reserved at the hotel. "If you want to meet smart people, learn about hacking, have fun with friends, hear some good talks, broaden your horizons and expand your knowledge," claims the conference webpage, "then DEF CON is where you should be." "Seriously," the page adds, "there is something for everyone to do."

The conference may claim something for everyone, at least everyone interested in computer security, yet it also sorts people into a hierarchy. The unwashed masses. The novices. The true believers. The inner circle. The leadership. Like most social organizations, it uses relatively simple means to divide people into classes. It gives badges to participants that distinguish the wearers as speakers, press, organizers, or exhibitors. It offers awards to identify the senior members of the society.

Consciously or unconsciously, the DEF CON participants support these distinctions with simple actions. They often favor a uniform dress of black slacks and tee shirts. They communicate with one another using a slang that can be disdainful of outsiders, that is both highly inventive and sufficiently offensive to prevent its use in a publication such as *Computer*.

When the DEF CON conference was founded, the technical community was unsure about how it should approach the problem of hacking.

Because the participants are involved with an activity that falls at the edge of polite society, they sometimes enforce social distinctions with brutal means. "Use the Internet at DEF CON at your own risk," counsels the conference material. "You will be sniffed. You have been warned." Those participants who do not know how to defend their computers from skilled intruders will find that their machines have been invaded and disabled. Beyond any physical and monetary damage, such an attack will bring a social stigma to the victim. The names of individuals who lose control of their machines are posted on a display in the hotel called the "Wall of Sheep."

I needed only a few minutes to confirm that X was indeed a speaker at DEF CON. "A Hacker's Guide to Government Cybersecurity Strategies," Major X, Super Secret Bureau of Hacking, US Army. It was one of the few talks that did not have a video record posted on the Web, which relieved me. While I would have enjoyed viewing a former student's accomplishments, I was fairly certain that she had embraced the social conventions of DEF CON, including the uniform dress code and hacker slang laced with military-strength obscenities. We don't want our children to grow up. We don't want to admit that they know evil. We want them to wear their dress uniform and end every statement with a dollop of military politeness .

PASSING FROM INNOCENCE TO MATURITY

DEF CON actually knew evil at its founding, but it too has passed from an innocent childhood into an uncertain maturity. "I started DEF CON to be a party for myself, friends, and the technology underground," reflected the founder, who is known by his nickname of Dark Tangent. "It is not meant to be an everlasting event or a summer camp for every kid who owns a computer."

When the conference was founded in 1993, hacking was still a new phenomenon. The first public events of hacking, Clifford Stoll's *Cuckoo's Egg* and Robert Morris's Internet Worm, were barely five years in the past. The technical community was unsure about how it should approach the problem of hacking. "At present, there is no technological barrier that separates the explorer from the criminal," reported an industry panel. Furthermore, many were willing to defend the rights of those individuals who tried to gain access to systems. The "blame for breaches of security and infiltration of personal, private systems is sometimes placed on the owners of those systems for maintaining an attractive nuisance."

Even though the professional community had yet to develop a unified response to the issue of hacking, no one was willing to develop a graduate program for hacking or a professional society devoted to promoting the

subject. The only way that hackers could build a body of knowledge was to use informal means: papers circulated among friends, electronic bulletin boards, and surreptitious electronic mailing lists. One group made a surprisingly bold effort on Bitnet. They created a visible listserv for hackers but required all potential members to hack their way onto the list.

While we have romanticized the private circulation of knowledge, we forget that knowledge dies without an organization to support it. Without a human organization that can sift information and raise the gold from the dust, knowledge will die as rumor and innuendo overwhelm any truth that may be within our grasp. In the early 1990s, it was possible to collect a lot of information about computer hacking. However, much of it was not true.

The birth of DEF CON was marked not only by a lack of information about hacking but also by tight economic times. The recession of 1990-1991 was one of the first periods in which technology workers were laid off from their jobs. As a result, many young programmers were looking for work. "When I started [DEF CON] there were no real jobs for people our age in computer security," recalled Dark Tangent. Long-distance "phone calls were expensive. Unix was not free. The only people with good Internet access were universities and businesses, and PCs still cost quite a bit of cash."

Initially, DEF CON was a simple and informal activity, a place where people with common interests could meet and relax. As the years progressed, the conference grew, and as it grew, it acquired the trappings of a formal organization. "It requires more people to be involved in organizing the show," complained Dark Tangent, "more insurance to cover more damage, more planning, more Con events, and more volunteer staff to make things run more smoothly."

At one point in the early part of this century, Dark Tangent concluded, "DEF CON reached a point where it is too big for its own good." An organization may have a single parent, but it is sustained by a committee, even if that committee is known as "The Goons" rather than a more prosaic name, such as "The Planning and Budgeting Group."

If the Goons originally came from that 1993 generation of novice hackers, they soon learned the skills of mature leaders. The public information on DEF CON shows how its leaders reduced risks associated with the meeting, built an administrative structure to handle recurring activities, and started recruiting new leaders. "Don't spend all of DEF CON sitting on your laptop," proclaimed one webpage, "get involved."

While we have romanticized the private circulation of knowledge, we forget that knowledge dies without an organization to support it.

LOOKING FOR X

It is one thing to get involved in an organization that has socially acceptable goals, public officers, and financial records that have been audited by an accounting firm that is both solvent and free from criminal charges. It is quite another thing to be involved with a group that boasts of its connection to people of dubious intent, takes no advance registration, demands cash at the door, and seems to subscribe to a code of honor among thieves. Yet, against expectations, DEF CON is surprisingly open.

The website boasts a remarkable display of photographs of the event. Most are informal snapshots and are difficult to interpret out of context. Still, they contain a lot of information that could be used to identify participants. In a few cases, you can see someone trying to duck out of the photograph. In considerably more, you find people waving the photographer away or making an obscene gesture at the camera. You "need to be very careful when you take pictures of random people," warns the DEF CON information. "Often they get very upset about that and you may lose your camera or consciousness."

I looked through a couple hundred pictures to see if I could find any evidence of X. Even in those sessions that would have been of special interest to her, she was nowhere to be found. I had a brief scare when I thought I saw a familiar ponytail in a photo of a fairly bawdy and explicit conference social event, but a second photo showed that the woman was clearly not X. If she was at DEF CON, and I have to trust her word, she knew how to avoid the camera. Perhaps she didn't want to be identified with the hacker community. Perhaps she wanted that community to think that she didn't want to be photographed. Perhaps she was avoiding the camera because she really is a hacker.

After digesting the idea that X had spent a week at DEF CON, I asked her if she had learned anything.

"Not a lot," she replied. "Our unit knows most of the things that were being discussed this year. I did meet a number of interesting people."

"What did they do?" I returned.

"Tough to say," she replied. "I gathered that most of them did computer security for large companies, but we stayed away from such subjects. We only addressed each other by our handles."

"Handles?" I queried.

"Nicknames—Dead Man, Stretch, Stone in the Road, Bunbury."

"Bunbury?"

"To each his own," she replied.

At this point, I switched subjects and asked what interesting problems she had found in her work. She responded by talking about the recent hacker attacks against systems in Asia. The press had concluded that these attacks were coming from North Korea. "North Korea has expanded its 'cyber combat' unit in charge of intelligence gathering through the Internet," claimed a source in Asia. "The General Staff of the North Korean People's Army has for years been running what it calls the 'technology reconnaissance team' which consists of about 100 hackers, mostly graduates of a leading military academy in Pyongyang."

"Do you think this is coming from Korea?" I asked.

"No," she said. "I don't think that they are that good."

"Where are they from?"

"That's the problem," she replied. "A lot of things that we see are coming from a single IP address in China. They're making no effort to disguise the origin."

"So either they are being brazen or someone is doing a good job of making you believe they are being brazen."

"Of course," X replied, "And they could easily have been at DEF CON."

David Alan Grier *is an associate professor of Science and Technology Policy at George Washington University and is the author of* Too Soon to Tell *(IEEE CS Press/Wiley, 2009). Contact him at grier@gwu.edu.*