

Mainframes Redux

Type80 Security Software, Inc. Managing Director Jerry Harding reflects on three decades of involvement with mainframe computers.

Interviewed by M. E. Kabay, PhD, CISSP, Associate Professor, Division of Business & Management, Program Director, Master of Science in Information Assurance at Norwich University, Northfield, VT

Q: Tell us about how you came to be doing what you do?

A: In 1971 I entered mainframe computing and worked my way up the ladder. By 1978, I was a mainframe systems programmer on the MVS operating system. By 1983 I became a self-employed consultant and formed a company called Systems Technology Services, which specialized in mainframe operating systems. Around 1991, with the early commercialization of the Internet, I remember picking up the paper and seeing that a team of local hackers had been charged with disrupting AT&T services by moving a satellite; I also read in *ComputerWorld* magazine about a 21-year-old hacker looking for an honest job in Internet security. What struck me was the statement that "He would work for anyone who would not force him to cut his hair." So I contacted a friend who was a long-time official in a federal law-enforcement agency and asked why the government wouldn't hire him. It seemed to me that if you wanted to examine your security, you would want to look at it with an open mind. But the government's hands were tied; they could not hire former hackers. So in 1994 Systems Technology Services expanded our services to facilities security, information security, corporate counter-espionage as well as continuing our mainframe operating system support. But the core focus shifted to information security through education.

Q: The reformed hacker was Chris Goggans. How did you know that he was reformed?

A: As in a marriage, I built a relationship of trust. To address the risks of hiring former criminal hackers, I used Chris only in education while we were building that trust relationship. Over the years, my trust has been rewarded and our working relationship has grown. I knew for a fact that Chris was working as an engineer, first with the Internet provider UUNet, and then with Wheel Group, which was marketing NetRanger, the first

commercial IDS. A funny aside, by the time he worked with Wheel Group, Chris had cut his hair down to almost military standards.

At the time, STS was sharing a small office in New York City and so we decided to put on our own conference for exposure. When we talked about security, we automatically thought of Washington; when we thought about break-ins, the Watergate Hotel came to mind. So in April 1994, we had our first conference: We called it "Electronic Privacy in the '90s." Keynote speakers were Stansfield Turner, former director of the CIA and Oliver North, former National Security Council staff member. Other speakers included Don Delaney, former Supervisor of NY State Police Major Crime Squad, Tobey Marzouk, a renowned attorney specializing in software piracy cases, and Jim Ross, a specialist in countersurveillance techniques.

The conference was very successful and so STS was offered challenging opportunities, one of which was to come to CNBC Studios in Fort Lee, NJ to film a segment on countering corporate espionage. The segment aired in August 1994 on a program called "Steals and Deals."

I was then contracted to do a counterterrorism study of the data centers for a Fortune 500 disaster-recovery corporation. We were also invited to present previously-unknown hacker technology to NATO Counterintelligence at The Hague in The Netherlands. We also arranged a private internal educational session for law-enforcement at an electronic research facility.

In 1995 I was asked to locate a former KGB agent who specialized in compromising networks to speak at a private international conference. First and foremost, I had to notify federal agencies of my intent. Then I launched a letter campaign to the Russian consulate in New York; I was eventually referred to the Russian embassy in Washington and then to the Ministry of Technology in Moscow. It was a two-year process that produced no results. However, persistence prevailed and I was eventually introduced to a former CIA employee through a mutual friend; he had Russian contacts. I met with the president of the Association of Former KGB Intelligence Agents in Washington and that led to an appropriate speaker.

So from 1994 to 1998 we became a leader in highly specialized security education and continued to work with NATO Counterintelligence as well as offering public seminars in Norway, the UK, Ireland and New York City.

Q: I remember your calling me up to arrange for a day-long briefing to NATO Counterintelligence in Germany -- what a blast that was!

A: In 1998, along with Jim Settle, former Director of the FBI Computer Crime Unit, we were managing yet another conference in Germany when we started discussing how the intrusion detection market had a gaping hole in it by not including the mainframe in enterprise-wide security. So Chris and I laid down some basic requirements and drew up a business plan. I began to look for capital funding. But this was a period when all the capital was going to dot-coms, so we did it ourselves. We refined the architecture on the mainframes for host-based IDS and recruited Don Pagdin as developer. He is now Director of Product Development and Support.

Starting in 1998, we started a new company called Type80 (based on the IBM log file record for security events) to focus on security. We officially incorporated in 2001 once development of Release 1 of SMA_RT was ready.

Q: Tell us about what is special about your product.

A: You can get a lot of information from our Web site < <http://www.type80.com> >. But what's special is that SMA_RT (Security Monitor Alert Real Time) is able to detect possible security-abuse patterns, commonly called signatures, that are not normally detected by looking at isolated log files or single images of the operating system.

Q: What do you mean by "single images?"

A: A mainframe can be divided into several logical partitions. Each logical partition runs an instance of the OS. If you have several CPUs and several logical partitions, you must examine the security across all of the logical partitions in order to determine a true picture of the security situation.

For example, consider real-time online password guessing (as opposed to offline attacks). There are ways to compromise passwords through patience and through knowing the rules for the environment's security systems. Unlike other mainframe security software, the Type80 security software does not interfere with events; it simply reports on the events when they happen and delivers a notification to the enterprise-wide SIM (Security Information Management), SEM (Security Event Management) or threat-management system (IDS).

Q: So if I understand you correctly, you have extended IDS functionality to include information from mainframe logging.

A: Correct.

Q: Where do you see information security going in the mainframe field?

A: The role of the mainframe is changing. It has become the enterprise server -- the server in the sky. IBM has invested billions of dollars in the future of LINUX on mainframes. In addition, US federal government regulations are going to require consolidation of enterprise-wide syslogs. One of the problems is that the MVS systems programmers are all retiring now -- or dying off -- and the support for the technology is being lost.

Q: Which leads us to the next question: What is being done about this?

A: IBM has launched project ELIZA to make the IBM operating systems self-maintaining, self-reliant and easy to install. They are initiating projects to re-introduce mainframe technology into the university curriculum. If I were a student today, I would give serious consideration to studying mainframes.

One of the obstacles to continued evolution of mainframes has been the cost of software. Typically, it has been acceptable for a mainframe software vendor to supply solutions with price tags of over \$100,000 and the software was priced according to computer size, speed and number of users. What is happening now is that all the leading vendors are rethinking this strategy. They are starting to charge on a per-usage basis. You pay only for what you use. This approach increases the ROI. Type80 has always charged this way from the very beginning.

Q: Please elaborate on why mainframes will be increasingly valuable -- and in which environments? Why should anyone bother with what many people have dismissed as the dinosaurs of the computer age? We are talking about wearable computes, infinite connectivity, and ubiquitous computing. Now you're telling us that gigantic centralized computers are good?

A: Yes. Not all companies have been successful in getting the right response time from client-server technology. So they are seriously looking to bring the applications back onto the mainframe. In addition, IBM has reintroduced the VM (virtual machine) which allows

thousands of instances of LINUX to run concurrently on a mainframe, eliminating the cost of replicating hardware by using virtual storage on a mainframe.

Q: I think this is analogous to what we naturally do in network management, where virtual circuits and datagram routing protocols allow us to share resources on demand instead of fixing them in place. Thus, the mainframe can allocate resources to fork an instance of the operating system for a user or group of users on demand instead of forcing the organization to buy hardware that may sit idle for a good deal of the time.

A: Yes, and we see significant cost savings as a result.

Now I want to jump back to security. I see the introduction of anomaly detection as part of the solution. We have reintroduced anomaly detection in a basic format in our software. I was doing some research recently on anomaly detection and ran across some work by SRI in the 1990s when they were asked to develop anomaly detection software for the FBI's internal networks. The product was successful, but at that time the FBI employees were trusted and well-behaved and so the product never actually had any anomalies to detect. It never made it into production.

Since then, the world has changed. Employees commonly move from company to company; the level of trust has dropped. It is for that reason that Type80 has incorporated anomaly detection into their product. Mergers and acquisitions sometimes result in disgruntled employees who have access to corporate systems. User IDs are often ill-maintained and access privileges are commonly copied from one user to another, allowing users to have unreasonable access. The merging companies may not have compatible security systems; for example, in the IBM field, the top security products are RACF from IBM, ACF2 and TopSecret, both from Computer Associates. The mainframe security people are forced to take on additional responsibilities and required to do more work with fewer people.

Another interesting development is integrating PKI with the mainframe. PKI leads to single sign-on, which leads to a single password to single point of failure and the possibility of massive system compromise through a single mistake.

In general, the mainframe security people and the network security people don't talk to each other. We need to fuse technology between these groups and a knowledge transfer so they're speaking the same language.

At Type80, I put together Chris Goggans from outside the box and Don Pagdin from inside the box and we've fused the technology from inside the mainframe and allowed it to report to the enterprise watchdog that normally focuses on the network. So we are integrating information from the mainframe, LINUX, UNIX and Windows systems as well as network components.

Q: OK, as my last question, do you think that we will see anything approaching the rigor of mainframe operating security filtering down into the personal computer operating systems and thus reducing the widespread vulnerabilities to malicious software?

A: Yes, but you have to understand that IBM and the mainframe operating systems have been doing this for 40 years. The technology is solid. It may take a while before this kind of strength is integrated into the client systems. We may not see a replica of mainframe security, but it would be a natural progression to see this kind of security reaching the desktop.

Source: Ubiquity, Volume 5, Issue 13, May 26 - June 1, 2004 <http://www.acm.org/ubiquity/>