Interview with Mark Loveless

RIK FARROW

Mark Loveless—aka Simple Nomad—is a security researcher, hacker, and explorer. He has worked in startups, large corporations, hardware and software vendors, and even a government think tank. He has spoken at numerous security and hacker conferences worldwide on security and privacy topics, including Black Hat, DEFCON, ShmooCon, RSA, AusCERT, among others. He has been quoted in television, online, and print media outlets as a security expert, including CNN, *Washington Post, New York Times,* and many others. He also knows They are out to get him. ml@markloveless.net

Rik is the editor of *;login:*. rik@usenix.org

I first met Mark Loveless online, which is appropriate. We were both part of a discussion group of journalists and hackers, although I didn't fit neatly into either group. Over time, I learned some things about Mark, mainly that he was best known for Novell Netware security tricks and hacks.

We had met in person a couple of times in the past, but then I learned that Mark was speaking at Enigma 2019 [1], and we planned to get together a couple of times for dinner. I learned a lot more about Mark, some of which we can reveal here.

Rik Farrow: Do some people still call you by your hacker name?

Mark Loveless: Most people who have gray hair call me Simple Nomad.

RF: When you started your career, were you interested in security?

ML: When I started, the security elements of it were more of a hobby. I liked those elements of it, but I never in a million years expected that's where I'd end up. I kinda fell into it.

My dad brought home an Apple II, because he was a big computer nerd who worked on mainframes, and that's where I started. First cassette tapes, then floppy disks after a while. My dad had formed a warez group with his friends at work. They would buy some software, and my job was to crack the copy protection.

RF: You were a teenager?

ML: Yeah. This was the last of the '70s to the early '80s, and I got really good at it. You could call up these companies and get developers on the phone. I talked to both "Steves" at Apple, but I was more excited when I called the Infocom people who did the game Zork. They were, to me, rock stars. I even talked to Bill Gates once, after I had gone back and forth with their support. Gates said, "You're an idiot, why are you doing it that way?"

RF: LOL!

ML: "I'm a kid, I don't know anything," I said. It's not like they were teaching us anything. In college, I got mainframe assembly and used punch cards. That's where I grew up. I got better at it over time.

RF: Where did you start working?

ML: American Airlines, a job at the help desk. I didn't have the on-paper experience for anything else. I had dropped out of college to be a famous rock star and needed something that would pay the bills. So I just went through the whole technological upheaval. My first experience from the Novell Netware was there.

I worked on the Sabre software, used by travel agencies for reservations, and what that included was a Novell server and some nodes. A lot of the nodes were diskless and booted off the network. There was a gateway machine, with a floppy drive, so it could talk over X.25.

My dad got a modem, and he had an X.25 account. So not long after that, I could use his account. I slowly began to know about how all of Sabre was working. I moved from Oklahoma to Texas because I got a job consulting, working with travel agencies. And that's where this all really took off. I got a lot of exposure to a lot of technology at that point.

I soon moved over to the railroad, Burlington Northern at that time, which later merged with Santa Fe Railroad.

RF: What a lot of people probably don't know is that railroad right-of-ways is where a lot of our communication infrastructure is buried.

ML: Right. This goes back to Civil War times. Wherever they are putting in rail, railroads are putting in telegraph lines. If someone else wants to put up telegraph lines that cross their right-of-way, the railroad can say that you have to hook up to our stuff if you want to cross the train tracks. As a result, the railroad got very smart: we'll just run extra cable along all our tracks, and they would lease this cable to communications companies. At one point, Sprint would advertise their *pin drop* network, that was so quiet: 50% of that ran on Burlington Northern networks. Next, people moved to fiber.

Even though "railroad" seems archaic, you picture coal-fired locomotives...the railroads have a lot of infrastructure. They had the largest IBM mainframe outside of the US government.

RF: You were working with Novell at AA?

ML: Yes, but it was also big time at the railroad. I had been on BBS and hacking forums, and it seemed that everyone was specialized. I noticed there wasn't much on Novell Netware, and I decided to focus there. I had access to some huge servers and huge installations, and there were test systems I could play with too.

RF: That's great.

ML: You could do really fun stuff. That was my introduction to running UNIX I had legitimate access to.

RF: This is in the '90s?

ML: Yes. The railroad had 35,000 employees plus union workers and no security department. It was me and my boss who became the security department.

RF: Many companies don't want security, as they prefer to "keep things simple."

ML: The weirdest thing we ever ran into was a department's mainframe program where the passwords were just four characters and we wanted to increase the length to eight characters. They came back and said, "We have union workers, we know what their typing rate is, and they are doing data entry. We don't want to waste keystrokes. We also have your help desk statistics, and we know how long it takes to do a password reset. Based upon what we think the number of password resets will be, moving to an eight character password will double the help desk workload." They had also calculated the amount of time it would take to type in the *extra* four keys based on the average of their users' typing ability.

We ended up doing a compromise. "How about six characters and we'll buy your department Post-It notes for a year?"

RF: LOL!

ML: Done! We had to spend part of our budget on Post-It notes for inter-office bribery. We printed up Post-It notes with the number of the help desk and "Do not write your password on this" printed on them.

That's what security was like back then. Portions of upper management would wonder, why do you even need passwords? Everyone knows our rates as we are required to publish them because of the DOT.

RF: So they weren't worried about someone coming in and changing all their rates?

ML: Exactly! But obviously, the thing that really cemented the security department in the company was when we had a virus outbreak and it affected hundreds of computers. We manned a hotline and came up with a battle plan. We would have a war room, we would fix this. We gained a lot of street cred, so to speak, from that.

I was still doing research on the side, the Novell Netware Hack-FAQ, and all that stuff. NMRC.org is still technically up and running.

And I was finding security bugs in software we were evaluating and using internally at the railroad. I reported a bug to a division of Bindview Corporation.

RF: What was Bindview?

ML: Bindview wrote management software computer systems. They also had an Internet security scanner, and I found something in there. So I wrote them that I was going to disclose the weakness. They patched the bug, and they ended up offering me a job.

I was thrilled because the railroad was going to have me work 12-hour shifts because of Y2K. By then the security department had grown, so it would me and one other person working round-the-clock, 12-hour shifts, for two weeks straight. Of course, nothing happened, but I left at the beginning of December.

At that point, I had been Simple Nomad on the Internet. The railroad was familiar with that Simple Nomad guy, and they could care less. They said just keep it separate, because I was helping secure their systems. I didn't report anything I knew about that would endanger the railroad. Or I would make certain that things were patched before I'd go public with it. They were very cool about it.

RF: Could you talk about responsible disclosure? You worked a lot with Novell.

ML: Novell had a reputation with hackers. Back in the day, they did this thing with a couple of Russian hackers who reported bugs. Novell hired the hackers, had them sign nondisclosure agreements, then fired them. The NDA were lifetime NDAs, which meant that Novell didn't have to patch what the hackers had found. They weren't US citizens, so what the Russians did instead was to pass the information to me, because I had a website.

So I was very wary about contacting Novell. And I was keeping my identities separate.

One time I contacted Novell by email, telling them that I've got this flaw, and I wanted to talk with them on the telephone about it. They say okay and gave me an 800 number. Being the paranoid hacker type, I knew that even though I could suppress the ANI, the automatic numeric identifier, what is now called caller-ID, in local exchanges or normal long distance, they could get the calling number because the receiving end of the 800 number was paying the bill. I decided that I was not calling on that 800 number.

Novell was using a PBX system, called Meridian Mail, and I had sort of a zero-day for that system. I could dial in, go through a sequence of numbers and steps, and I would get a dial tone, so I could dial out. I would use a computer to handle the sequence, and then I could call long distance for free from that PBX. I used that trick with Novell. I called up the PBX, dropped out to a dial tone, looked up the number of the security person using the Meridian Mail system, then called him up. I asked him for the extension for the conference call, and to him it appeared I was calling from an internal number. "Where are you?" he asked, and I answered, "I'm in Texas." I got the number for the conference call.

I was paranoid that Novell was going to do something.

RF: Because of what Novell had done to the Russian hackers, this seems likely.

ML: I reacted to that. Sometimes Novell employees wouldn't leak bugs but would say "Look at this."

RF: They would point you in the right direction.

ML: Correct. I had problems with other companies too. Microsoft at the time was weird about stuff when you reported it to them. I tried reporting something to ISS, who had a security scanner, and they got really weird about it. We just backed away from that. We were doing this on the side as a hobby, and they wanted us to present our disclosure policy signed with our PGP key. And that just seemed too weird.

RF: You worked for MITRE, the defense contractor that publishes the CVEs for bugs. What was that like?

ML: Weird. I did work on standards like CVE and CWE mainly, and dabbled in a few other standards. But a lot of what I did also involved working for the security department responsible for answering to attacks against MITRE's systems. That group only dealt with APT attacks, and that was some eye-opening stuff. I can't go into much detail, but I can expand on some general concepts. Most of them were Chinese APT groups; we would refer to them as campaigns. We tracked dozens and dozens of individual little things from phishing email subject lines, various IP addresses, recipient lists, compilers used to compile backdoors, and on and on, and patterns emerged. We actually didn't really care *who* was attacking us per se; we mainly wanted to know if we'd seen them before so we could anticipate their next move.

Granted, there were all kinds of clues that most of the attacks were Chinese sponsored, but I had tons of friends in the security community saying, "APT is made up, people can fake their IP address, it's not the Chinese, and APT isn't real." I'd have to bite my tongue since most of the proof that it was, for example, Chinese sponsored was from classified briefs and whatnot. I mean I had a security clearance.

I think the one I hated the most was the argument that these attackers didn't live up to the "A" part of APT. They weren't "advanced." I'd hear from friends that "they don't use zero-day all the time, so they aren't advanced. I'd be using wicked cool zero-day." Oh no, you would not. My background was in hacking—I was breaking into systems in my youth—and you *never* wasted a zero-day on a target unless you really wanted in there and all of the low-level stuff didn't work. It was like these people who were "playing offense" by doing penetration testing really thought they were actually hacking.

Hackers, and these APT actors as well, did not have Statements of Work to not attack production systems or to limit themselves to a two-week engagement. No, hackers and APT actors would cheat, commit felonies, take months and months to get in, hit production systems, lie, intimidate, steal, whatever. When you reverse engineered an APT backdoor and found your internal DNS servers' IP addresses hard-coded into the exe, you knew you were dealing with someone advanced. They'd been in before, they knew your internal network layout, and so what if they

didn't use a zero-day to get in. Advanced meant they played serious and played to win at any cost. At times I wanted to punch some of my friends in the mouth. "Not advanced" my ass. Now of course it is all out in public, and everyone accepts APT as real.

I remember my first classified meeting and how disappointed I was. I mean everything said in that meeting I'd already known well before working there. I think the only thing I didn't know was the fancy names of everything. Goofy code names. I was like shit, so no reverse engineering UFOs or something?

Speaking of which, I had no idea how I got a security clearance. I'd been under investigation by more than one government agency for hacking, and they still approved my DOD-sponsored security clearance. I know this in part because a few years earlier the NSA tried to recruit me, and I stated, "I can't work for you, I have a file, I've been investigated," and they were like, "Well sure, we've read it, and yes, you'll never work for law enforcement, but you can work for us, we're the good guys, we're the NSA." They actually said that, "We're the good guys." Whatever, I turned them down.

Truthfully, the most interesting work I did at MITRE was all classified, and I can't talk about it, but it was some really cool stuff. However, it was nothing to do with UFOs unfortunately.

RF: Also, you worked for Duo Security. What did you do for them?

ML: Yeah. After MITRE I went to Duo Security. The idea was Dug's (Dug Song, the CEO) that we form a Duo research group and do security research like the old days—make it fun and entertaining. Get content out and speak at conferences, do press interviews, all that. We'd be smart security people doing cool stuff who happened to work at Duo Security.

In essence we were doing a form of marketing. The Marketing Department loved us; well, we were probably an ass pain to work with, but once we got to know each other we had a blast. I loved working there, the product was cool, and if you were at a conference wearing a Duo shirt people would run up and tell you they loved you and would want selfies with you.

Originally the plan was to IPO, and they even were hiring C-levels with that in mind, but then the Cisco offer came in and that ended that. Many of us were heartbroken, since Cisco is a huge corporation with a radically old-style corporate infrastructure. Sexy, cloud-based startup to a division of an old school corporation. Sure they were trying to go a lot more modern, hence the buyout, but it still hurt. By then the focus was on making Duo look both attractive and useful to Cisco's bottom line, so my Duo job rapidly went away. I had the opportunity to work in one of several Cisco departments, but instead I left. I wanted to work some place cool like Duo used to be.

I did the "funemployment" thing after Cisco and started blogging and whatnot. I probably could have done that for a year or so since I had my buyout money. Not a lot of money but "forget working for a while" money. Then I got a call from Kathy Wang, whom I've known from the hacker and security conference scene for nearly two decades, and she told me about GitLab, and it sounded too good to pass up. Plus the employee base is 100% remote, all cloud-based corporate infrastructure, so it has a modern and forward-thinking unicorn startup vibe and everyone is pretty damn awesome. I had to go for it.

I just started there, and I'll be working on research in areas where my skills are, and doing other stuff like conferences, blogging, and whatever. It's nice to work at a place that is extremely open and really heading in a good direction. I am still going to blog and speak at conferences, and life should be a lot of fun.

Reference

[1] Physical OPSEC as a Metaphor for Infosec, Enigma 2019: https://www.usenix.org/conference/enigma2019/presentation/loveless.

Submit Your Work!

FAST'20

18th USENIX Conference on File and Storage Technologies

Sponsored by USENIX in cooperation with ACM SIGOPS
Co-located with NSDI '20
February 24–27, 2020 | Santa Clara, CA, USA
www.usenix.org/fast20/cfp

FAST brings together storage-system researchers and practitioners to explore new directions in the design, implementation, evaluation, and deployment of storage systems. Interested in participating? Paper and tutorial submissions are due Thursday, September 26, 2019.

nsdi '20

17th USENIX Symposium on Networked Systems Design and Implementation

Sponsored by USENIX in cooperation with ACM SIGCOMM and ACM SIGOPS
Co-located with FAST '20
February 25–27, 2020 | Santa Clara, CA, USA
www.usenix.org/nsdi20

NSDI will focus on the design principles, implementation, and practical evaluation of networked and distributed systems. Our goal is to bring together researchers from across the networking and systems community to foster a broad approach to addressing overlapping research challenges. The Fall deadline to submit paper titles and abstracts is Thursday, September 12, 2019.