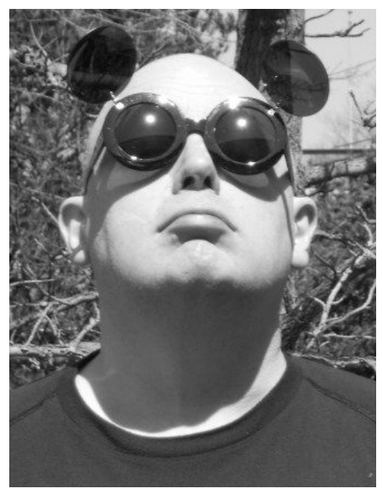
AN • INTERVIEW • WITH

Michael W Lucas

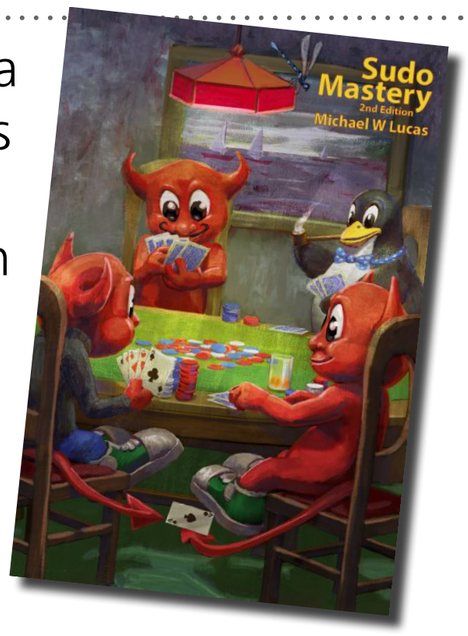
by Allan Jude and Benedict Reuschling

This is excerpted from BSDNow, Episode 329, recorded December 2019. Allan Jude and Benedict Reuschling interview Michael W Lucas.



BENEDICT REUSCHLING: Michael W Lucas has been interviewed on this show a couple of times. His last interview was a few months ago, and we thought you might like to know what he has been doing and what he has planned. Here's the interview. Enjoy!

REUSCHLING: Welcome, Michael! You released a new book recently that I'm sure listeners would like to hear about. Can you tell us a bit about that book? It's about sudo, I hear.



MICHAEL W LUCAS: Well, thank you for having me. And yes, the new book is a second edition of *Sudo Mastery*. Sudo hasn't undergone extensive changes unless you're using LDAP. But it has undergone a lot of minor changes, so, basically, this second edition is about catching up on that and making sure that the information is accurate for today's sudo. I also dove deeply into some changes in the recommended configuration. For example, sudo has features like checksum verification to make sure binary hasn't been tampered with. And, of course, nobody is going to go and compute to checksum of every binary by hand, let alone update them whenever they're patched. So, I did some scripting for popular operating systems to programmatically compute the checksum for everything.

REUSCHLING: Oh, that's useful.

LUCAS: It can be. If you suspect your system is vulnerable to outside tampering, checksumming may be a solution for you. And there are some new calls out there. They used to have a tool to transform a sudoer's file into LDAP format. That was handy and useful, but now they have a general tool to transform sudoers to and from LDAP and then to and from JSON. So, you can put your sudoers in any format you want. You can feed it to your auditing program and make sure that everything is the way you want. And, of course, the book has a beautiful cover.

JUDE: It does! Will you explain the different versions of that wonderful cover?

LUCAS: If you buy the e-book, you get a very nice cover based on one of the classic "dogs playing poker" image. And since people have asked, yes, there's a reason one of the BSDs is wearing a black turtleneck. And the reason another BSD is slipping him an ace.

If you get the paperback, you'll get a more complete version of that, and hardcover wraps around on the cover. If you have the hardback, the dust jacket has art continued onto the inside flap. So, if you're looking for something fun and pretty, this book will do it. I'm really pleased with how it came out.

JUDE: So, you have cover art that comes in bigger and bigger and bigger sizes. What are you going to do next?

LUCAS: I've been pondering what comes next. I'm not exactly at a loss because I have lots of ideas. But I just finished a really huge project with the jails book [*FreeBSD Mastery Jails*]. I had to write six books to write the jails book. It was a giant project, and everything was aimed at a particular destination. Plus, I wrote a couple of little books on the side as I was treading through it. I no longer have a master plan, but I'm trying to come up with an overarching goal. And whatever I do in terms of art, books, what have you, will feed into that. So, I do have some ideas, and thanks, but I'm not asking the whole Internet to send me suggestions.

REUSCHLING: It might be too late now!

JUDE: Speaking of the jails book, almost everyone who uses FreeBSD could learn quite a bit from it, even people like me who have been using jails and FreeBSD for years. There's more stuff in the book than in my head! Were there surprising things you learned while writing it?

LUCAS: I've been using FreeBSD since late 1995 and doing that work forced me to go back and review everything I knew—and some things have changed since 1995. I learned a lot of little edge cases on filesystems. You can really do some amazing things with DEVD, and even nullfs is useful. It's amazing how fine-grained some of the controls are in jails now. I remember when System 5 IPC in a jail was simply not a thing, and now you can turn it on and off per jail and even turn on System 5 IPC features individually per jail. That's something I know was implemented because people needed it, but I'm sort of afraid to find out why someone needed System 5 shared memory—but not semaphores.

JUDE: Yeah, I think part of that was back in the past when the IPC name space was all one—you maybe want a jail to be able to only see parts of it. Although a number of years ago when we finally got namespacing there so you could have Postgres in two different jails that wouldn't accidentally stomp on each other, it maybe became less of an issue.

LUCAS: I thought that at first, but that feature evolved later. So, this was some sort of design decision. I trolled through 20 years of history, and the order in which things happened was really illuminating. It's a great example of iterative development. I mean jails saved me a lot of pain back in 1999, 2000, and they've just crept forward over the decades. Jails are hard is the short answer. They are the culmination of everything in systems administration. You must know filesystems. You must know upgrades. If you have a lot of jails, you really have to have some sort of orchestration or automation. This stuff gets very complicated very quickly because all of a sudden you could run 500 virtual machines on one host. You have to manage 500 virtual machines on one host. And that's just terrible. Nobody wants to do that.

REUSCHLING: Many people will end up grabbing the book when they are in need of a jail.

LUCAS: Yeah. It's out there. People who need it will find it. People who don't need it, well, they have a simpler life than the rest of us.

JUDE: Oh, you know, I've gone overboard with the things you can do when you combine ZedFS and jails to the point where I needed a system where customers need to be able to upload files but need to make sure they can only upload their own files and so on.

LUCAS: Yes. Anything like that I would certainly put in a jail. Anything that faces the public I want to put in a jail.

JUDE: Yeah, it's really interesting how well ZedFS and jails fit together, considering, on one hand, that Sun, when they developed ZedFS, integrated it with zones, which are kind of like jails. But they're also quite a bit different, and the fact that we've managed to make it line up so well I find really pleasing.

LUCAS: It is nice, and I think the issues that apply to getting a virtualization aware of a filesystem are not unique to zones. They simply set up a filesystem that can be delegated and that can have lower-level permissions.

JUDE: It's really interesting that you can do both. You can jail a dataset, which basically means you're delegating it to root in the jail. But then root in the jail can delegate to an individual user in that jail.

LUCAS: It really is lovely.

JUDE: Um-hum.
REUSCHLING: There are use cases that you typically don't think about at the beginning, but then you're like, yeah, it's possible and I can see a good application for it.

LUCAS: Yeah, really, systems administration is about looking at the tools you've got and figuring out how to plug them together to solve a problem. And ZedFS is a great tool.

JUDE: So, moving on, how did you come to the realization that the world was in need of a book about Simple Network Management Protocol—SNMP?

LUCAS: Oooohhhh. Because it's everywhere and none of the existing books thrilled me. And SNMP is really not as hard as you might think.

REUSCHLING: Well, that's what the S is for, right?

LUCAS: Yes, yes. And the truth is that the actual protocol is very simple. It has seven parts—that's it. The problem is with what all of the vendors and implementers have done with those seven parts. And no matter how specifically you write the standard, there is always room for interpretation. What we need is not a book on how glorious it is, but a book on "these are the pieces, here is where we are, and here is how you figure out this stuff."

When it works, it's fantastic. People use SNMP to monitor all the time. SNMP is well-suited for managing networks. Even today in talking to people and doing the research, there are folks who say if you have a really saturated Internet link, you may need to issue a command to a remote device to solve the problem. We have SNMPv3, which a lot of people are scared of. After digging into it, really, I think we're just teaching it backwards. Sometimes it is the only solution you have, and I would not suggest that you build your whole network around SNMP. But I would say it's a tool you need to know whether you're a network admin or a sysadmin. Sometimes you need that particular tool, or a tool will solve things that are really hard to solve in other ways. There's so much confusion about it.

JUDE: Yeah, you know, it's definitely a tool in my toolbox, and I am not shy to admit that I didn't ever really learn it properly. I just kind of muddled through enough to get what I needed out of it.

LUCAS: Yeah, and you can discover the information you need in two packets.

JUDE: Right. When I am running that every 30 seconds, it's a lot nicer than having something much more heavyweight.

LUCAS: Mind you, I have learned things like you can run SNMP queries over SSH.

JUDE: Ohhh!

LUCAS: Which I'm not covering because the book is already too big. But it is a possible solution for some sorts of problems. If you have a certificate authority infrastructure already, you can run SNMP over TLS.

JUDE: Does that still go over UDP or does it change to TCP in that case?

LUCAS: It can use either. DTLS is TLS over UDP.

JUDE: Yeah, for datagrams.

LUCAS: There are a lot of options there. If I can successfully orient people so they can separate learning the protocol from learning a vendor's weird configuration, it'll be more than worth it.

REUSCHLING: What else did you learn about SNMP during the research for the book?

LUCAS: Well, everything is terrible, but that's not a surprise. Let's see. A lot of people have done interesting things with it. There are agents from MYSQL and Postgres and Apache that will plug right into net SNMP. So, you can easily pull statistics from all sorts of software. There is extending it. You can have SNMP run arbitrary commands on your server. Which may or may not be a good thing depending on how complicated you want to be.

JUDE: And graph trends and all kinds of stuff.

LUCAS: Oh, yes, yes. Of course, the problem with monitoring things like that is you don't need to monitor them until they go horribly wrong—I love system administration!

JUDE: Looking back, how did your planning for the year work out?

LUCAS: Well, I had all sorts of things I wanted to do. About a year ago, they took out half my thyroid, and all of the mysterious health issues I've had for the past few years cleared up. And this is great! This is fantastic! It meant I could do everything. And I had to learn once again the hard way that I can do things, but I can't do everything. I planned to write a bunch more words than I did. I accepted too many invitations to travel, and travel messes me up. So, I've decided to do less travel and more books. I make words for a living. This is what I've always wanted to do. I'm very lucky to be able to, and I just have to stand here at my keyboard and do the work.

JUDE: Well then, speaking of that, can you tell us what you're planning?

LUCAS: I've got a couple of thoughts on tech books. The DNSSEC book is due for an update. And with DNS over HTTPS becoming more of a thing, that should probably go in there as well.

JUDE: Especially now that we're in an age where most people are using it and don't understand this stuff.

LUCAS: Yes.

JUDE: People are making an informed decision to use DOH.

LUCAS: Right. It's a great immediate solution for people living under censorship regimes. However, authoritarian and censorship states don't put up with those kinds of problems for very long.

JUDE: Yeah, and I think the most dangerous part is that it's not the whole solution. If you depend only on it, you're going to run into problems.

LUCAS: Yes, yes, quite a few problems. But I can do a book on how to set it up. And email could be an interesting book. There's really nothing on how to set up a complete email solution these days. So, that's a possibility.

JUDE: Yeah, doing DKIM wasn't too bad, but the newer DMARC stuff was very confusing to me.

LUCAS: I think email privacy is mostly lost. Even if you run your own mail server, chances are you are communicating with someone who uses one of the big commercial mail companies. But it's still worthwhile trying to run your own mail servers, and that's a topic I've been looking at. And I'm starting to ponder a couple of OpenBSD things—and anytime I mention writing an OpenBSD book, people jump up and want the next Absolute OpenBSD. Let me say there are no definite dates for that—I'm glad you want it, and it will come.

JUDE: What about the sequel to *git commit murder*?

LUCAS: That is on my list. I tried writing it while I was very ill. Right now, I'm pushing to get the SNMP book done. The nonfiction brings in the money, and I'm glad I have it. I'm not knocking it, but I do not have enough novels out to make a living by writing *git commit* books. I will be very happy when I'm finished with SNMP.

REUSCHLING: Any final thought today, Michael?

LUCAS: I say thank you to all the people who buy the books and that I'm glad you find them helpful. Also, if you've managed to listen to this interview and me babbling on this long, thank you for that too.

REUSCHLING: Thank you, Michael, for your continued writing and your books.

P.S. Today, Lucas finds his statement about traveling less disturbingly prescient.