Keeping FreeBSD Secure: Learn the Whys and Hows with the FreeBSD Sec Team

BY PAM BAKER AND ANNE DICKISON

We all know the scene. The room is dark, with the only light provided by the laptop screen. The hooded figure is typing furiously at the keyboard. Suddenly, lines of symbols, letters, and numbers fly into the terminal window as the nefarious character smiles brightly. They. are. in.

But not so fast! The dogged security team has been planning for this. Protocols are in place. The breach is secured; the sinister hacker is captured; and of course, the world is saved. Ah, MovieOS. Don't you just love it?

Now we all know in the real world, trying to keep any type of technology secure is nearly a herculean task. Strengthening security for the FreeBSD Operating System is no different. But we wanted to know more about exactly what the FreeBSD Security Team does and why they do it. So, we sat down with Gordon Tetlow, a volunteer FreeBSD Security Officer, and Ed Maste, Deputy Security Officer, and Mark Johnston, a FreeBSD security team member. The latter two are sponsored by FreeBSD Foundation and support the security team in both ongoing operational aspects of the team's work, and proactive development.

Q: What is FreeBSD Project's overall approach to security?

Ed Maste: The security team focuses on several different aspects of security within FreeBSD. One area is what's often called a PSIRT, or Product Security Incident Response Team. This is a main focus of the security team today.

This team fields reports about vulnerabilities and issues and responds by identifying the problem and managing the release of the fix. Examples may include errors in drivers or pro-

tocols, bugs found by our own proactive fuzzing efforts, other automated tools, and code review. The team's response includes preparing or integrating patches to fix those issues, preparing and publishing security advisories to notify the community of the issue, and deploying binary updates.

A second focus area is proactive security work, which includes targeted efforts to find issues, vulnerability mitigations that reduce the impact when issues do occur, and general architectural security review. These efforts were historically undertaken directly by the security team. In the current security team model responsibility for certain areas has moved to separate groups of subject-matter experts. FreeBSD's random number generation subsystem is an example of one such area — the security team remains involved, but specific responsibility is delegated.

Proactive security work also includes ongoing code review and auditing, following security reports and discussions in other projects, fuzzing and test failure analysis, and related areas.

And a third area is the security of the FreeBSD infrastructure itself, meaning the FreeBSD website and source code repository and all the services that we run. In these cases, there are other groups within the project who have primary responsibility, while the security team may offer advice and review.

Proactive security work also includes ongoing code review and auditing.

Gordon Tetlow: The other role that we play is in coordination with industry efforts. There are vulnerabilities that affect more than just the FreeBSD project, where there is common code shared with other open source projects. We end up with industry-wide efforts to address those. An example would be OpenSSL, which is another project that we incorporate. We have to coordinate disclosure and coordinate patch response for that.

And then we do much the same all the way upstream, too. One example is when Intel had the "Spectre" and "Meltdown" speculative execution issues a couple of years ago. Literally everybody, every operating system manufacturer, and a lot of other folks all had to get together and coordinate an industry-wide response, for better or for worse. We play an important role in that broad industry response.

Q: What is FreeBSD's specific role in disclosures?

Ed Maste: If we have a vulnerability reported in FreeBSD that we will be addressing, we handle the public disclosure to the FreeBSD community of that vulnerability and handle the patch and binary update for the fix.

We also are involved in public disclosure in terms of coordination with industry partners and peers. If there's an issue that affects Linux and OpenBSD and NetBSD and FreeBSD, for example, and someone is coordinating the reporting of that issue with all of the different communities, then we'll collaborate with those other projects to help make sure that the fixes are released on the schedule set by the vulnerability reporter, or the industry peers who are managing and coordinating the issue.

Q: Do you have formalized roles, or a mission statement or charter guiding your security work?

Ed Maste: Quoting from the FreeBSD project's "Administration and Management" page,

> The FreeBSD Security Team (headed by the Security Officer) is responsible for keeping the community aware of bugs, exploits and security risks affecting the FreeBSD src and ports trees, and to promote and distribute information needed to safely run FreeBSD systems. Furthermore, it is responsible for resolving software bugs affecting the security of FreeBSD and issuing security advisories. The FreeBSD Security Officer Charter describes the duties and responsibilities of the Security Officer in greater detail.

Gordon Tetlow: The security officer has an open-ended charter to make things secure, which includes the ability to override actions and decisions of other developers, if necessary, in the name of security. Now that's not something that we exercise lightly and it's definitely something we have to be very conscientious about using. But the charter mandates that we ensure, by whatever means necessary, that what we're doing is the right thing.

Q: How are reports on security advisories handled? Can they be anonymous and protected?

Ed Maste: We provide guidance on the FreeBSD website that describes the policies, the order of the approaches that the sec team follows, security advisories, and other helpful information.

Gordon Tetlow: Note the section "When is the security advisory considered" right on the front page for the security team. For people who are interested in reporting security advisories, there's also documentation on how to report a security advisory. That's listed kind of as a subset to that.

People can send us regular or PGP-encrypted email to secteam@FreeBSD.org. What we want to let people know is if they're wanting to get in touch with us on a sensitive issue, they're welcome to encrypt the data to us. That way they can know that only a certain couple of individuals would be able to read it.

The security officer has an open-ended charter to make things secure.

Q: How else do you find security issues?

Mark Johnston: We aim to find security problems proactively, in addition to addressing vulnerabilities reported by third-party researchers. We try to be proactive and responsive to all situations that arise.

In my case, it's largely just about day to day working on FreeBSD, looking at bug reports and user submissions and also doing my own testing. We have several developers in the community who spend most of their time doing nothing but testing FreeBSD and reporting bugs. Upon further examination like this, you might find a security vulnerability lurking in there, even if the person reporting it isn't aware of the security implications.

I spend a lot of time drilling down into those kinds of reports and looking for something that might be more serious than it appears at first glance.

Ed Maste: Mark also worked to bring the Syzkaller code-coverage-guided system call fuzzing tool to FreeBSD, and worked with the project's maintainers to have it run on a consistent basis. Syzkaller performs automated kernel fuzzing in order to find inputs that lead to a kernel crash or some inconsistency detected by instrumentation. Syzkaller's reports may indicate potential vulnerabilities, but in any case represent bugs to be fixed. Mark worked on increasing Syzkaller's code coverage, triaged its reports, and has fixed many issues as a result.

FreeBSD also has a stress testing suite, called "stress2", which can find race conditions or misbehaviour that occurs under high load. A number of kernel bugs have been fixed as a result.

Ed Maste: Among the useful cases that Mark identifies out of the general bug reports mailing lists, social media and other channels are issues that people have reported that they want fixed. Quite often they're unaware of the potential security impact of that problem. We try to understand and extend evaluation of the problem to include any potential security impact and act upon it as warranted.

The security officer has an open-ended charter to make things secure.

Q: What's next for the security team?

Ed Maste: There are both technical and operational improvements we're looking at within the security team. We currently have focused efforts to discover potential issues via fuzzing and other tools. We intend to continue and increase this effort, for example by extending Syzkaller to include additional system calls, increasing code coverage.

This has been ongoing for some time, but we expect to increase our effort in revisiting system defaults, and applying sandboxing, privilege reduction, and other user space techniques to software in the base system and the ports collection.

Operationally, we are looking at improving coordination with downstream projects and vendors who use FreeBSD as the basis for their own development. We also need to keep working on bringing new members into the security team; this is a challenge shared by many open source projects.

A prolific and versatile writer, **PAM BAKER** writes on many topics for leading tech and science publications. She is also the author of many dead tree books, ebooks and white papers. Her latest book is Decision Intelligence For Dummies which is about a new way to mine data and use AI in decision making. It was released in February 2022. Baker lives in Atlanta, Georgia where she's currently working on her first sci-fi novel.

ANNE DICKISON joined the Foundation in 2015 and brings over 20 years experience in technology-focused marketing and communications. Specifically, her work as the Marketing Director and then Co-Executive Director of the USENIX Association helped instill her commitment to spreading the word about the importance of free and open source technologies.