H D Moore

October 01, 2014

Who are you, and what do you do?

My name is H D Moore (since the day I was born, it doesn't stand for anything). I am a security researcher and the chief research officer for Rapid7. Some folks may be familiar with my work on Metasploit, but these days I also spend a lot of time scanning the internet as part of Project Sonar. My servers send friendly greetings to your servers at least once a week. Howdy!

What hardware & operating systems do you use?

Lots. My normal workload involves crunching a billion records at a time, running a dozen different operating systems, and still handling corporate stuff via Outlook and PowerPoint. As of 2009, I finally made the switch to Windows as my primary OS after being a die-hard Linux user since 1995. That doesn't mean that I use Windows itself all that much, but I find it to be a useful environment to run virtual machines and access the rest of my hardware with SSH and X11. The tipping point was the need to quickly respond to corporate email and edit Office documents without using a dedicated virtual machine or mangling the contents in the process. The second benefit to using Windows is on the laptop front; Suspend, resume, and full hardware support don't involve weeks of tuning just to have a portable machine. Finally, I tend to play a lot of video games as well, which work best on overspecced Windows hardware. All that said, Windows as a productivity platform isn't great, and almost all of my real work occurs in web browsers (Chrome), virtual machines (VMWare for Intel/AMD64 and QEmu for RISC), and SSH-forwarded XFCE4 tabbed-terminals.

The laptop I currently use started life as a banged up ASUS ROG G750 (17") bought as the display model from a Best Buy. The drives, video card, and memory were swapped out bringing the total specs up to 32Gb RAM, a 512Gb SSD boot disk, a 1Tb backup disk, and a GeForce GTX 770 GPU. This runs the most loathed operating system of all, Windows 8.1 (Update 1) Enterprise, but it has a huge screen, was relatively cheap, and can run my development virtual machines without falling over. It also runs Borderlands2 and Skyrim at maximum settings,

critical features for any mobile system. Given that the total cost was under $1,500, it is a great machine for working on the road and blocking automatic weapons fire (as its weighs about 20 Lbs with accessories). I carry this beast around in a converted ammunition bag, sans the grenade pouches.

On the non-portable front, I tend to make Frankenstein monsters by taking HP workstations with bare specifications and then gutting and replacing most of the components. Their 8XX-series workstation chassis are tool-less, support CPU water-cooling, and generally make hardware swaps a breeze. HP's component prices are astronomically high and I usually source those elsewhere for my builds.

My primary desktop is a HP Z420 with a single Xeon E5-1620 (watercooled), 64Gb of RAM, and 2 x 256Gb SSDs in RAID-0 as a boot disk, with a 4Tb backup drive. I use 3 x 24" IPS LP2475w monitors in a vertical + horizontal + vertical configuration, which matches my typical workflow of an open web browser, a productivity screen (terminal, documents, etc), and another screen dedicated to email and IRC (stacked vertically). Vertical monitor orientations are highly underrated, especially for reading and writing large amounts of content or code. A Nvidia Titan drives these displays and runs oclHashCat and cudaminer for DogeCoin on occasion. This box runs Windows 8 Enterprise most of the time, but I boot into alternative environments as needed. My network connection from this desktop is 2 x 1GbE bonded connection to a "prosumer" switch that connects the rest of my servers. I use a Cherry "clear" switch clacky keyboard (the WASD) most of the time and my original Model-M when I need some ear-splitting noise to emphasize intent (eg. when writing advisories with great anger and furious vengeance).

Most of my archival data storage is handled by a Synology NAS with 12 x 3Tb disks. This also uses a bonded 1GbE pair to the primary switch. The data stored on this system isn't particularly sensitive (rainbow tables, huge archives of public content, research datasets, etc), but I wouldn't recommend this platform from a security perspective. Synology tends to be slow to patch and often has bone-headed security issues in their OS builds (enabling the VPN used to enable a backdoor root account).

My data processing, development, and password crunching all runs on a mismatched pair of HP workstations.

The first machine is a HP Z800 with dual Xeon X5690s (watercooled) and 96Gb of ECC RAM. Storage is all over the map, with an Adaptec RAID card, and two RAID-1 volumes (2x2Tb, 2x3Tb), and a RAID-6 volume (4x3Tb). There is also an 8-bay eSATA chassis connected and I use this to hot-swap datasets and generally make copies and backups of whatever I am working on at the moment. Occasionally I stuff the eSATA bay with SSDs when I am working with a system that needs fast random data access but doesn't fit into RAM. This box runs Ubuntu and handles most of my day-to-day development. I keep a mini-clone of this system as a virtual machine for my desktop and my laptop. The desktop environment is XFCE4, but I primarily interact with it using X11-over-SSH. Network connectivity is also bonded 2 x 1GbE.

The second machine is a HP Z820 with dual Xeon E5-2687Ws (also watercooled) and 200Gb of ECC RAM. This box has 4x3Tb disks, partitioned into RAID-1 for boot and root and RAID-0 for data access. Using relatively slow drives, the RAID-0 data partition still yields about 600M/s read speeds (sequential), which works really well for large-scale data processing. Between the two CPUs, this machine has 32 hardware threads, and I try to keep the load pegged at 30+ by using it for data mining, password cracking, and various other research tasks. The great thing about having 200Gb of RAM is that even for large processing jobs, code optimization is rarely needed to get the results you need in a usable timeframe. I use this system to prototype analysis tools before actually having to care how well they perform. This box also has a pair of Nvidia GTX580 GPUs for CUDA work and supporting password cracking and mining efforts. Just like the previous system, connectivity is bonded 2 x 1GbE, and it runs Ubuntu as well.

My router runs Ubuntu on an Intel NUC (v2 i5) from a plain old SSD. My home network is split up by VLAN to isolate my wireless and target environments from my work systems. This router connects to a trunk port on my main switch, which VLAN tags traffic from each of ports, including my two internet links. The primary link is a 1Gbit/1Gbit from AT&T and this falls back to a 10Mbit/1Mbit cable link whenever a butterfly flaps its wings in China and the AT&T connection dies. Once Google finishes their Austin rollout, I plan to move to dual Gbit and use some fancy routing policies to load balance these connections and handle upstream failures.

On the furniture side, I use a powered desk that can be raised and lowered, and managed to source an elliptical office chair before Skymall started selling it for four times the manufacturer's price. I still spend most of my time sitting, but at least I can get my brain moving on a slow day

by pedaling along. I tend to dismantle and rip the piezo speakers out of anything near my working area and put stickers over anything that is blinky. I have enough dislike for random blinky and beepy things and that I tend to go medieval on devices when rectifying a distraction.

Outside of production systems, my office is piled high with random ICS, SCADA, and consumer networking devices, many in various status of disassembly. I have a working area for current targets and a "plastic bins of crap" management system for the rest of it. Complimenting this is a shelf full of diagnostic and debugging toys, ranging from JTAG adapters to a milspec thermal camera. I keep DeconGel and other industrial cleaning agents around for when projects go wrong (bits of broken lead solder from older gear, etc). Nearly everything in my office was sourced from and will return to the junk-hacking scrap heap that is eBay (or my local Goodwill, depending if it is useful to regular people). The weirdest functional systems in my office include a working Tadpole tablet running VxWorks 5.5 and a Tru64 system running on a "blue board" DEC Alpha AXP that has manual wire patches to fix its CPU socket.

I tend to use GPE-compatible Android mobile phones with S-Off (for +1 nerd points) and generally break them every 3-6 months, possibly as an excuse to buy the next one. I keep a bin of dead mobile devices around as target practice for Metasploit modules. A large portion of my life is dedicated to memorizing and entering 6-digit MFA codes for a couple dozen applications, something my current phone (a Nexus 5) does a reasonable job of assisting with.

And what software?

I use Chrome as a my primary browser and spend a lot time staring at Pidgin, Skype, Google Hangouts, Outlook, and the rest of Microsoft Office. In terms of getting actual work done, I live in either Sublime Text 3 or XFCE4's Terminal and VIM. Standard tools include RVM, Ruby, VMWare, QEmu, IDA Pro, and the security triad of Wireshark, Nmap, and Metasploit. Password cracking is still John the Ripper (--fork=32 ftw) for most things and oclHashCat as needed. My shell is **still** Bash (damn you Zsh hipsters, get off my lawn!). Git and Github are invaluable for not just managing code, but tracking projects via Wikis, and generally managing the research process. For data analysis, I love the GNU utilities (sort --parallel -V -S 128, egrep, wc -l, parallel, xargs, etc) along with a couple tools built at work, such as a DAP and Recog.

In my free time, I spend way too many hours playing games that could be most generously described as monkey traps for nerds (MMOs, horribly complex and unforgiving RPGs, etc). If am looking for something that requires less math to play, it tends to be UT2004, Quake3, or Goat Simulator (yes, it's a thing, imagine Tony Hawk as an invincible goat, without a skateboard, played by a drunk five year-old). That tends to be it from a software standpoint. There are other tools that I pick up for specific jobs, but I like writing my own tools, and anything I have to do at least twice ends up being a Metasploit module at some point.

What would be your dream setup?

I pine for a dual-OS environment that didn't require compromises on performance or security. I would love to be able to have a locked-down Windows install for work, another for video games, and a Linux desktop for everything else, all tied to the same keyboard, mouse, and displays. I tried solving this in the past through a hodgepodge of virtualization, KVMs, and software tools like (the probably still buggy) Synergy2, but nothing that exists today matches my requirements. There are hardware solutions that get close, but they sacrifice basic things like copy and paste to get there. PCI passthrough still doesn't cover the gaming uses cases for GPUs properly. If I had one wish, it would be solving the dual/triple environment problem. In a perfect world, something like Qubes OS would enable PCI-passthrough on GPUs and make a complex, multiple operating system environment secure and performant.

On the laptop front, I would love for someone to emulate the now-defunct Sony Vaio Z series laptops, but deliver a coder-friendly keyboard and a Linux-friendly hardware configuration. The "chiclet" keyboard of the Vaio Z2 made me want to **HULK SMASH** trying to write out anything significantly complex. My hands look like they belong to a rejected claymation model, so tiny keys don't work so well. The Eurocom Xeon "laptops" look nice, but given enough network connectivity, I can always rely on cloud and home-hosted servers for when I need a lot of processing power, and I don't necessarily need a high-cardio workout just to move my laptop through an airport.

Server-wise, RAM is relatively cheap, but servers that are quiet and have ridiculous numbers of DIMM slots are far between. The perfect server has 1Tb of RAM to use as a working memory and a 10Tb+ of SSDs for storage and snapshotting. CPUs are basically "fast enough" given a parallel-friendly load, but a quad-Xeon with 20 cores per CPU (like the E7-8870) could

definitely improve my workflow. Doing all of that on a budget is definitely a challenge and even clustering smaller systems tends to get expensive on one axis or another (energy, heat, repairs, etc).

Regarding mobile devices, I am pretty happy with how fast the industry is moving, although I wish AOSP and other pure open source efforts would pick up more mindshare. The amount of data leakage on mobile devices is just frightening and there are very few things the average consumer can do to reduce these leaks without giving up on modern conveniences. Phones are finally fast enough that you can do interesting things with them, but I still miss tactile keyboards, and most mobile devices are really designed for consumers of content, not creators. My perfect phone would run a quad-core CPU at 2Ghz, have a slide-out keyboard, have 4Gb of RAM, support dual-SIM, and provide at least two SD card slots along the edge for easy data management. For a cherry on top, the baseband and operating system would be open source, easy to audit, and make it simple to prevent data leakage from untrusted applications. As Microsoft seems to have figured out with Windows 10, people want their mobile devices to be useful computers, and not their computers to act like brain-dead mobile devices.

In terms of furniture, I tend to change my setup pretty often, or at least adjust my desk height, and swap between standing, sitting, and pedaling the elliptical while I work. I wish there was a curved 80" monitor and software to handle the mapping properly, while still allowing unique sections of the display (tiled or otherwise) to be dedicated to an application. I spent a lot of time moving windows around and trying to optimize my workflow across three monitors. I couldn't do it with a single monitor without significant help on the software side (ratbox for Windows or the equivalent). Maybe VR headsets will eventually be a viable option, but they still have a long way to go on the resolution front.