

Secure & Portable Persona Management Version 3.0

The internet is becoming increasingly dangerous for everyone, and in particular there are targeted attacks aimed at activists and organizers. If you are running a specific persona for any reason, say interacting with a specific social media community, it's probably best that you compartmentalize it from your other activities by encapsulating it in a purpose built virtual machine.

Virtualization

The right way to do this on Windows would be to purchase a copy of VMware workstation, but that's a \$99 expense. VMware offers a free introductory product known as VMware Player that also suits our purposes, as long as we apply a few usability tricks.

Be aware that VMware products require a processor with certain minimums and you'll want a lot of ram. ATOM and Pentium M processors won't do the job, so smaller laptops are likely not capable of running such software, and a gig of ram is a very tight fit. A new machine in the \$500 range with an i5 or i7 processor will do what is needed.

If you have an Intel Mac there is a \$79 product called VMware Fusion that will host Windows or other operating systems as well. There is also an Apple only product known as Parallels and this is reputedly a very solid option.

Operating System

You will need a copy of Windows. We have a slipstream of Windows XP – it's got drivers needed and the serial number is already embedded. This will NOT behave if you try to install it using the quick install. You have to create a blank VM, then bind the CD ROM to an ISO of the Windows install disk, and don't forget to delete the SCSI disk that the system defaults to and replace it with an IDE drive.

You can also build your captive operating system with Linux. We keep a copy of TAILS, a hardened, readonly version of Linux in which all applications are configured to use TOR, for truly radioactive environments. Coupling a TOR only virtualized OS with a host OS running a VPN is proof against a variety of ills in the world today, and the subject of another write up of ours entitled Double Secret Internet.

Privacy & Portability

The whole idea is to encapsulate an online persona in a safe environment. The VM is the container for the personality, but what if your laptop is stolen, or if you're arrested and questioned?

We run <http://truecrypt.com> software to make encrypted file containers. Our first test involved creating a 4 gig space, binding it to drive W:, and installing Windows in a VM

there. The persona in the VM is now perfectly safe if the machine is lost or stolen, so long as a strong password is used.

There is also a portability and restoration angle to this. If you build a VM on this drive W: it's actually inside a file, say windows-xp-base.tc, a TrueCrypt volume. Copy that file to persona-1.tc, then persona-2.tc, and so forth. You can bind each to drive W:, fire them up, configure them for the appropriate persona, and you've still got windows-xp-base.tc available if you need to restore due to a suspected virus or create another persona.

The encrypted VM files are large, but they're not a hopeless case for trading via a fast cable modem connection.

Graphics

The one of the key reasons people move from VMware Player to Workstation is the fact that Player has less graphics capabilities. We have some fairly limited needs so we can work around this.

The solution is fairly simple. Install TightVNC on your VM once Windows is running, connect to it from your desktop, and you can pick the resolution you need. This isn't going to work for graphics intensive programs, but we're just wanting to corral a web browser in a safe place, and a remote desktop protocol should keep up with this limited use. This also solves the context switching problem – no capture of the mouse pointer occurs when switching from one's desktop to the captive system.

IP Address Concealment

The most basic means of IP address concealment is to install The Onion Router (TOR) and the bundle of tools that come with it. This system is slow and it counts on endpoints that are often blocked by sites we wish to visit. A commercial VPN provider is often a better solution, so long as the vendor is chosen with care and attention is paid to the host country of the endpoint. This can be run in the virtual container or on the host OS itself.

There are many service providers that offer VPN services. Most have a slow or limited transfer free mode and then a paid service that funds the operation. We've evaluated a few of them and we need to do so again in the context of this project, seeking one that can be auto started on boot, so that the source address the machine is using is cloaked before any programs are started.

Perhaps the best plan when using a virtual OS that might be compromised would be to have the commercial VPN provider of your choice already running prior to booting. There is room for improvement in the operating discipline suggested here.

We tested Hotspot Shield in our initial build and it seems to work fine, but it requires that you recall you need to start it, and only protects browser traffic.

Cyberghost VPN provides a “start with Windows” option and this has behaved for us so far in testing.

We see others using WiTopia. Associates of ours have purchased and liked this service.

Some diversity in VPN solutions is desirable. If everyone who uses this settles on the same service that means banning a handful of IP addresses functionally shuts everyone out. We probably need to figure out how to provide our own endpoints using a rotating set of VPS in other countries, but that’s a job for the infrastructure people.

Personality Concealment & Failure

This can not be stressed strongly enough: we have only protected against the following threats.

- Disclosure due to loss/theft/seizure of host computer
- Disclosure due to spearfish or other compromise of browser
- Disclosure of IP address due to log examination or subterfuge
- Monitoring of traffic by your ISP or a compromised machine on your network

You might face a loss or theft, you could run into a technically advanced opponent, but it is almost certain that if you try to approach a venue where you are already known by an existing name or pseudonym that you will get “made” in short order.

You have habits that include:

- The time(s) of day you are active
- The language you speak
- The situational knowledge you have when interacting with a certain group
- The software you prefer to use
- Quirks of spelling, punctuation, and other subtle hints as to identity
- Whatever objective you have in approaching the venue

The following are some failure modes we've personally experienced over the years:

- Used a pet phrase from a persona in a venue we frequented - instant outing
- Used bit.ly link shortened from a known account via Twitter – instant outing
- Disclosed specific software preferred during conversation, not a full outing but it brought scrutiny that made the effort fail eventually
- Use of phone number that had a single obscure Google hit – instant outing.

We often feel we're being clever in constructing a persona but we generally fail miserably due to time constraints. We're always goal oriented when in character and that is an instant tell to those with situational awareness. If you don't have time to "be" someone else and remain in character your results will be limited.

Shared Context & Record Keeping

Those who do this a great deal develop various record keeping schemes. If you're just trolling around with no serious concern of consequences a collection of Google Docs can serve as a repository.

We assume if you are reading this you're a bit more on the down low and are storing your records in encrypted form. Again we like TrueCrypt – an archive of a megabyte in size is easily emailed and you can fit quite a lot of text files in a container that size. Stick to text if at all possible – fancy packages like Microsoft Word leave a broad trail of not so obvious marks on anything that might escape into the wild.

Keeping a coherent view of what has happened is hard when you have one life and one persona. We've used the following at various times for various purposes:

- Storybook novel writing software – single user, text only storage inside, but can effectively track multiple personalities and themes on a timeline. Choose this one if you're just getting started, as it will foster your art as well as your science.
- Web Brain – powerful mind map facilities, no sense of timeline, team functions permit easy sharing. Contents are discoverable if you use the web sync, stick to BrainZips in encrypted containers for safety. \$300/seat and \$75/year.
- Maltego – Open source intelligence collection platform, heavy on data visualization, mostly for Twitter-centric things. \$650 first year for a proper license, but much can be done with the free Community Edition.
- Sentinel Visualizer – industrial strength social network analysis/data visualization with temporal and geospatial analysis. You have to really want the lulz to throw the \$2,500 entry cost to In-Q-Tel venture DMS Advanced Systems Group.

Motivation & Futures

The whole concept of persona management was getting a lot of attention during 2009 when I was still active with Project Vigilant. There were a bunch of half baked solutions going around, really expensive things that I felt would only serve to train smart opponents as they watched their less swift peers fall for the subterfuge.

Fast forward to 2012 and now the internet is so toxic I've corralled my actual social media presence in a couple of VMs to stick a wrench in the constant profiling and intrusion attempts, and those VMs live on a machine that doesn't touch anything important. There is a lot of drag as I move stuff back and forth, certainly, but I'm not keen on uninvited visitors.

More and more Twitter and Facebook serve only as channels for introduction and venues for public theater. Anything of consequence has vanished into OTR encrypted chat, or SILC servers, and new contacts have to run the gauntlet of my quizzing those who introduce them, then getting them on the phone so there is a voice and a callable number to go with.

A sloppy social network only betrays maybe 25% of what is important to an intruder lacking subpoena power. Merely adopting the operating discipline implicit in what is suggested here and both your signal and trail will drop dramatically.

Commit to trying to run a persona for a while if for no other reason than to understand what will and won't work; your situational awareness will be dramatically enhanced. Stick to it until it becomes second nature and you can simply disappear when needed, or protect your friends from unwanted attention with a fog of disinformation.

You have the natural rights of free speech, free association, and free assembly. There are many private entities, from the lone obsessive stalker to the largest corporate entity that will interfere in all three of these fundamental human rights.

You commit a courageous, moral act when you do these things we suggest, leaving those who do not respect you pounding their keyboards and crying with frustration.