# Pwned by the Owner: What Happens When You Steal a Hacker's Computer

Content:



*Dr. Andrew Zoz Brooks, a well-known computer expert and co-host in 'Prototype This!' TV series, shares his hilarious computer theft story with Defcon attendees.*

Alright, I have no less of an authority of speaking at Defcon than Jason Scott here. Everyone is really confused about what room I am supposed to be in, and the talk should start, like, a few minutes late.

So, to fill in some time before I get started, I thought I'd just tell you a little story about my other experience with computers and the police, which was soon after I got to MIT (Massachusetts Institute of Technology).

You know, you get to MIT and this is kind of pulling hacks ethic: like, doing these pranks to amuse people. So you start immediately looking for things to do. And I noticed outside my lab across the street there was a manhole that had been opened and there were some lights in it and some power cables tangling, like extension cords, and it sat there like that for weeks.

*VT220 terminal – part of the experiment*

And, you know, what the hell is going on? There weren't even, like, cones around the manhole to stop people from falling in; it just sat there. We were like: "We don't know what's going on here, but maybe we should turn it into a hack." So we got an old VT220 terminal and decided we would set it up on the edge of the manhole with a lamp as though some hacker had, like, popped out of the manhole and was up to no good with their VT220 hacking or, you know, whatever that was in the manhole.

And we would film it, we'd set up a camera on the 7th floor of the building next door and film what was going on to see if we got any good reactions. So we go down, you know, about 8 pm or something, it's dark in Boston at 8 pm; and we set up a VT220, a little desk lamp and everything to make this kind of set up.

Then we go back in and take the elevator up to the 7th floor to set up the video camera. And that was the fatal error, because by the time we'd got up to the 7th floor office to set up the video camera, the cops had already arrived and were staring at this computer wondering what was going on.

We are looking at the cops looking at this computer, and then suddenly for no apparent reason they just start kicking the shit out of it. And one of the cops picks up the keyboard and key caps are flying everywhere. And were just like: "Oh my god, why didn't we set up the video camera? This is like Rodney King for computers right here."

So, we learned 2 lessons from that: firstly, always set up the video first; and secondly, we started fantasizing about what else we could have done, because after they finished beating it up, they loaded all the broken parts into the police car and they took it off who knows where.

And we thought: if only we had some kind of radio transmitter hidden in that VT220 so we could hear what those guys were saying. What did they think it was? What kind of totally evil computer break-in to this manhole, just probably like sewer or a steam tunnel, could have been going on?

So, second lesson – recordings: audio, video, get a radio link, because you just never know what's going to happen, even with the police, they're very unpredictable. Ok, I think I can now get started with my subject.

## How It Happened...

You guys have all read the title of the talk, so you know the basic gist: my desktop computer got stolen out of my place. There have been a lot of stories lately about people who had their computers stolen or their iPhones stolen, and have recovered it. They recovered their laptop because they clicked the iSight and they retrieved the picture of the person, and they've got the Where's My iPhone feature and stuff like that.

> *What happened was a straightforward physical security fail.*

But this is not a mobile piece of equipment, doesn't have a camera in it, so the situation was a little bit more complicated. And the circumstances of the theft – I just have to confess, what happened was a straightforward physical security fail.

My place is on the second floor, there are three locks in between. I rate everything in terms of zombie defense, so my keys are coded in terms of danger of zombie access, so the green key is the outside, the yellow key is the second floor and then the red key is my room.

But, unfortunately, we're not dealing with zombies in this case; they climbed through the second floor window via an access method that I hadn't noticed, and then busted the red lock, so just had to bypass one door. It's the kind of thing where that whole situation could have been prevented with a 20-dollar deadbolt, so that's worth keeping in mind.

*Stolen Macintosh with backups*

The upshot of it was my Macintosh, which was a Quicksilver G4, my pride and joy, was now gone. I'm the kind of person that keeps religious daily backups. In fact, I kept religious daily redundant backups. Unfortunately, both of those were stored in the same room as the server and were also stolen. Lesson: off-site backups.

These days I dumped everything onto a portable hard disk and gave it to my parents in Australia and said: "I hope I never need to ask you for this back, but I might one day."

It's very-very traumatic to me: I lost all my music, all my photos, all my video projects. So I had to channel that energy into trying to find my machine. I get very angry without my heavy metal.

## Learning the Machine's Location

*No success searching eBay and Craigslist*

What I did have was the serial number of the machine and the stats of what machine it was, so I started to look for it in the kind of usual places you would think someone would dispose of a machine: I started searching eBay and Craigslist for months and I didn't find it. Fuck!

*DynDNS Updater – might help*

Someone asked me almost immediately when it got stolen: "If it gets plugged back into the network, will you be able to find it again?" And I thought: "Yes, I'm running a DynDNS Updater. It will update the domain record and I'll see it again!"

And then I thought about it a bit more: "Well, the machine is set to auto-boot into single user mode. So my data security policy at that time could definitely have used 'work'," and I thought: "Well, the guy could boot into it, but it's not going to get back on the network, because I'm pretty sure the network settings are locked and it's on an intranet, so the thief is not going to be easily able to reconnect it to the network, unless they happen to have an intranet with the same settings as I did – unlikely." So, fuck!

Even with my legendary stubbornness, I eventually gave up looking for the machine on sale sites and trying to get people to go to places for me. I was in San-Francisco filming "Prototype This!" at that time, and I was trying to get people in Boston to go to flea markets for me and look for it, and they're telling me to fuck off, as you would expect.

*DynDNS account expiration warning email*

So, alright, time passes. Now, if you use DynDNS and you use the automatic updating service, if you don't update it for a while you start to get messages like this **(see image)** which say: "Your account looks inactive, so you can either just let your account be deleted or you can click on this link and reactivate it."

I would click on these links once a month, because I thought: "Why set it up again if I start using it again?" And at some point I noticed something; I thought: "That's funny; I don't remember getting one of those emails in a while. I wonder what's up with that."

*DynDNS host update log*

So I log into DynDNS and there I see: holy shit, 2 years later that domain record has started to be updated. What the fuck? So, I quickly nslookup the IP, and… pretty interesting: my machine that was stolen in Boston now seems to be on a cox.net dial-up in Las Vegas **(see image below)**.

*nslookup*

So I called the cops right away, and they said: "Oh yeah, we'll subpoena that IP record." And I said: "Well, you've got to make sure that you get a historical record for this, because this is a dial-up, a dynamic IP, it's going to change a lot, it's going to be totally worthless if you look it up now and it's not assigned to anyone or it's assigned to someone different." And, sure enough, they came back a month later with the subpoena results that said that the IP address wasn't registered to anyone. No shit.

## Remote Access Fun

*SSH did the trick*

I wasn't staying idle in the meantime waiting for them. First thing I did of course was ping it and see if it was up, but it wasn't: you know, it's a dial-up, it's not always online. So let's do that thing a whole shitload all the time and wait for it to come back. And sooner or later it did come back. Let's see if we can still SSH into that box **(see image above)**. Fuck yeah!

*VNC works wonders!*

SSH is not the only service I'm running on that machine, I'm also running VNC, so let's see if that's still up **(see image)**. So, I can still SSH to it, I can still VNC to it; the machine has not been rooted, reformatted or locked down. But he did at least go to the travel of changing my desktop background, I'll give him that.

Now, this is a Macintosh, so we can enter things on the command line that make it do things: like, text a speech that comes out of the built-in speaker with no apparent window or source: "I am going to get you, motherfucker!"

## Retrieving the Burglar's Personal Details

But childish fun aside, I wanted that machine back, so let's start taking a look to see what we can find out about the guy that has it. He hasn't changed the names of my hard disks; there are some PDFs on the desktop – they look like forms for unemployment benefits in Nevada. It turns out they are

unemployment forms in Nevada, but they're not filled in electronically; they've just been downloaded and probably printed out, so that's a dead end.

*Burglar's photo 1*

*Burglar's photo 2*

*Burglar's photo 3*

But we have some stuff that are .JPGs. Hmm, maybe they're interesting pictures, let's take a look **(see photos above)**. So now, either whoever has this computer is really into saving photos from DiamondEarringWearingDouchebags.com or these are pretty hilarious self-portraits.

*Browser cookie file*

So, let's find out a little bit more about what this guy's into. Let's take a look at his browser cookie file **(see image)**. Here's an excerpt, here are some sites: we have Blackphatbooty.com, Bigbuttbrazilianmoms.com, Freebigassporn.org, Elephantasses.com, alright.

What are some searches? Alright, we got: 'sexy beautiful fat ass', got several searches for free porn, not something I thought was that difficult to find. But we're getting a psychological profile. I know some of you right there are thinking this is my machine and these are my cookies. Now, I swear to you that they're not; you're just gonna have to take my word for that.

We got some location information in these cookies – nothing we didn't know, it's all Las Vegas. But a little bit deeper here we find Gmail address. Thank you Google for keeping that stuff very easy to find!

*Retrieved profile of the thief*

So, what have we got? We got location in Las Vegas, we got a name, we got a face, we got a Gmail account, and we got a keylogger installed.

At this point I got sweaty pants, I'm like: "Oh, can't wait for this machine to come back online", because it goes offline typically 8 or 10 hours after it goes online – so, waiting to get that first key log back.

*Captured key strokes*

Here's some of the initial key log stuff **(see image to the left)**. So, right away we have a street name, but not a street number; could be his, might not be. We got one login and password, but we don't really have a lot here. There are a lot of weird key presses, and I know that he's using the Web a lot, because I'm watching also on VNC some of the time when I happen to be there when it's happening.

*Pwned!*

But how is he logging into things without typing many passwords? Well, the browser he's using is Camino, which is the browser I had installed, because he can't install new software since he doesn't have the admin password. And Camino is the Macintosh build of Mozilla. It's integrated well with the Mac OS Keychain for storing passwords. Now, the Keychain is encrypted. But he's storing his passwords in my Keychain and it's encrypted with my password! So, I download the Keychain file and open it in Keychain manager – and he's pwned.

*Birthday greeting from Army.com*

At this point I just need to find out a little bit more; I need a full street address, I need to find out maybe some more info about this guy. So, what about his birthday? Well, Army.com is nice enough to

send him a birthday greeting that tells us the day and the month **(see image)**, but what about the year? It's not in there. Well, maybe his logins and passwords can shed some light on the subject: Gmail: mrguzmanmel@gmail.com / guzman85; Facebook: timrican@yahoo.com / guzman85; Yahoo: timrican / guzman85; BlackPlanet.com: fricanpapi85 / guzman85; Mocospace.com: 1flyricanpapi / guzman85; eBay: mguzman1985. You think maybe he was born in 1985? Well, eBay tells us that he was.

*Getting a lot closer to the point, but street number missing*

But, you know, this guy is not using the same password for everything; like, I don't want to completely denounce his password behavior. He does mix it up a bit: we've got some twiddling on the numeric keypad going on for some of these.

So, what we have at this point is the name, and an address, and a birthday, but still not the street number. I kind of need that to send the cops around. Oh wait, some recent PayPal receipts **(see left-hand image below)**.

*PayPal receipt says a lot*

*Credit card account login page*

*Credit card client info*

And, you know, I don't want to send the police on a wild goose chase, I need some confirmation here. So I happen to be watching him logging in to his credit card account, over VNC one day. And isn't it a good thing that his bank's security is strong and he's got this image identifier that's protecting him from phishing attacks? **(See middle image above)** Doesn't it make us all feel warm and fuzzy?

But there we are, logged in, there's the address **(right-hand image above)**. That goes off to the police. But while the police are doing their work, let's take a closer look at this guy, let's get to know him a bit. You know, he's using my computer… Who is Melvin Guzman?

# Who is Melvin Guzman? The Close-Up

*The thief's Facebook profile*

Well, Melvin Guzman is the kind of person who spells his own name wrong on his Facebook page **(see snapshot)**. His main activity is taking photos of himself for online dating sites, and when he saves those pictures he just mashes on the keyboard. So, my stolen computer, my beloved Mac is being used by someone less competent than a typewriting chimp. But, you know, maybe if he'd stolen infinite number of computers, he might figure out if the complete works of Shakespeare could fit in a Mac OS filename.

But thanks to a self-portrait obsession, I hereby present the many sexy faces of Melvin Guzman **(see photos below)**. I'm sure the ladies love some of those. And all the ladies out there: this man is available, contact me if you would like his phone number.

*Facebook page main photo*

*Ladies must love this one*

*Wink-wink*

*Melvin in shower*

Now I'm sorry to anyone who wanted to see the full monty here **(see image on the left)**, but after I originally submitted the slides the Defcon stuff told me that they might have trouble when they put the videos of this talk on their CDs that they have for sale afterwards, and they may have some trouble with the A/V company if I left it in. So I had to search for something to cover up the weiner here, if you like.

*Making love to the camera*

But let me just say that when I searched for Defcon logo images on Google Images I only had to search for icon size. If you've ever wondered what photographers mean when they say: "Make love to the camera" – that's what they mean **(see collage on the right)**. Having made love to the camera he doesn't mind cuddling it afterwards.

But this seems to work, alright, because the sexy ladies of the Internet responded and it worked out for him, so here's what he was receiving back **(see pics below)**. So, at last he found the 'phat' booty he was looking for, I assume so.

*Melvin is popular!*

*She doesn't mind dating Melvin*

*Found it!*

*Why type different messages?*

I don't know a lot about online dating techniques, but I noticed when I was looking at the keylogger that there were a lot of Ctrl+V's. And I found out why that was from watching in VNC. This guy would write a message once and then copy and paste it to literally hundreds of women. I think this used to be called the 'shotgun approach', but I don't think they make shotguns that can hit 200 targets at once. So maybe we should call it the 'nuke from orbit approach'.

*Surprisingly, Melvin is a wannabe criminal justice expert*

And finally, an interesting bit of info considering that this is a guy using a stolen computer: he's taking an online course for criminal justice. I think he's enrolled in my online course for criminal justice.

After I handed all the address information I was able to give them, the police were able to go and recover the computer, and I think they did it the day after I submitted these Defcon slides after the deadline.

## Lessons Learned

*Conclusions to draw*

It taught me some lessons that I thought I would share with you. First of all, obviously, my security of the machine in the data security sense, in terms of not encrypting the hard disk and letting it boot in single user mode – was shithouse. But if I had better security, then I would never have been able to recover the computer: if the guy couldn't log into it, if he had to wipe the drives, if he couldn't reconnect it to the network – same deal.

So I actually recovered the hardware and I did recover some of my data; some of it had been erased but I got a little bit of it back and I set up rSync scripts every time it was online to pull in more and more of the stuff. I often wonder if he was paying for bandwidth as well, because every time it would connect I'd be sloping gigabytes of stuff back down his dial-up.

The second lesson is a lot of these services are potential vulnerabilities against a trained threat. Like, everyone here is thinking: "Oh yeah, you're running VNC, and if you're not tunneling it over SSH, you're totally making a mistake," especially also having a daemon that tracks the IP addresses wherever this machine moves, especially if this was a mobile platform. You know, if I was running a DynDNS update on my laptop, people would know where I was all the time. So that would be bad against a trained threat, but very good against a low-tech threat. So it's all about, sort of, threat modeling and remembering to buy that 20-dollar deadbolt.

> *The final lesson learned: don't fuck with a hacker's machine!*

Another thing: the Keychain[1] versus key logs. I'm one of those guys that never really trusted the keychain, because it's a single point of failure, it's got everything in it. What if you could get into it? But it's actually an interesting defense against the keyloggers, which is something you're more likely to have on your machine from spyware and stuff.

There are more sophisticated keyloggers; there are ones that log mouse movements and clicks and things like that; but for a very basic keylogger, having forms and passwords just fill themselves in automatically when you've logged in once – you know, it's potentially protective.

And then finally, having my serial number was great, like, being able to give that to the cops, file the police report meant that the hardware could be recovered; without that serial number there's no way. So write that down somewhere.

And then, the final lesson learned, of course, I'm sure you all know: don't fuck with a hacker's machine! Thank you!

---

**david b.**