

RE: Advice regarding servers and Wiping Drives after testing

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-09/msg00101.html>

- *From:* "William Holmberg" <wholmberg@xxxxxxxxxx>
 - *Date:* Wed, 12 Sep 2007 14:30:13 -0500
-

Hi Robert,

It is interesting that you point this out. One of the people in our local chapter told me there was a company or group of electronics people working on a "Drive level" SATA "Adapter" (for lack of a better word I guess) that would read the "top level" magnetic layer generated by the head on a particular sector, and exactly measure it's intensity, then generate an "inverse field" (not my words) which would effectively nullify that overwrite, leaving the last write before that one plainly readable (with some variables). He said it was an exciting prospect because since the head that last wrote the 1 or 0 was the one that "erased" it, it worked to a point of surprising the design team with it's ability to accurately reconstruct data overwritten.

How much of that was hearsay, fabrication, or wishful thinking, I don't know. He compared it to military sound suppression devices for helicopters, which (if you didn't know) can sample the exact frequency generated by the rotors and moving parts and generate an inverse frequency, out of phase with the original, through powerful Horn Drivers mounted under the rotors. The effect in sound engineering is a precisely controlled "OOP" (Out OF Phase) situation. You can experience it to a lesser degree very simply with your home stereo speaker. Simply exchange one of the speakers Red and Black connectors. The phase cancellation that occurs makes it very difficult to hear certain frequencies (depending upon that particular speakers dynamic range and other boring items) and in some cases can almost entirely cancel out each other across many frequencies.

Note: If you do this, do not turn it up too loud, because the other effect is that the speakers will be pulling "IN" when they should be pushing "Out", and the Coils can get damaged by bottoming out and inverse clipping. Horns should be unaffected however.

Thanks for all the stimulating conversation on this, as well as the fascinating reading materials.

-Bill

RE: Advice regarding servers and Wiping Drives after testing

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]
On Behalf Of gjgowey@xxxxxxxxxxxxxxxxxxxxx
Sent: Wednesday, September 12, 2007 12:52 PM
To: Ansgar -59cobalt- Wiechers; listbounce@xxxxxxxxxxxxxxxxxxxxx;
security-basics@xxxxxxxxxxxxxxxxxxxxx
Subject: Re: Advice regarding servers and Wiping Drives after testing

What you're forgetting is that these pieces of software aren't you normal "access the hdd through regular os calls". These pieces of software are sending low level commands to the drive its self an interpreting what's sent back instead of relying on a middle layer. They can literally have the head scan a particular sector as many times as is needed until it gets a signal back that resembles something useable. Writing all 0's will never prevent against software recovery because the all 0's approach is like recording over a used VCR tape once.

Geoff

Sent from my BlackBerry wireless handheld.

-----Original Message-----

From: Ansgar -59cobalt- Wiechers <bugtraq@xxxxxxxxxxxxxxxxxxxxx>
Date: Wed, 12 Sep 2007 12:48:42
To: security-basics@xxxxxxxxxxxxxxxxxxxxx
Subject: Re: Advice regarding servers and Wiping Drives after testing

On 2007-09-11 William Holmberg wrote:

On Tuesday, September 04, 2007 1:03 PM Ansgar -59cobalt- Wiechers

wrote:

On 2007-09-01 gjgowey@xxxxxxxxxxxxxxxxxxxxx wrote:

A since pass with all zero's really won't protect your data from being recovered by more advanced data recovery software let alone alone hardware.

I'd like to see a single case where someone was able to recover data from an overwritten harddisk, even after a single pass with zeroes.

No doubt you are an intelligent and well educated person in these fields, and probably have many areas of expertise more proficient than

RE: Advice regarding servers and Wiping Drives after testing

RE: Advice regarding servers and Wiping Drives after testing

mine. I do have to state however, and nearly any Infragard member can tell you, the FBI uses tools that accomplish this on a regular basis. I have no doubt other agencies do as well. We have had demonstrations of it remotely in a class I help instruct, SAFE computing for Law Enforcement and Non-Profits (SAFE is Security And Forensic Education) at Metro State University of Minnesota, MCTC campus.

Demonstrations of recovering data from fully overwritten media, without opening the case? Sorry, but I seriously doubt that. Feel free to prove me wrong, but without evidence I find that really hard to believe. Keep in mind we're not talking about wiping single files, but overwriting the entire media.

Regards
Ansgar Wiechers

"All vulnerabilities deserve a public fear period prior to patches becoming available."

---Jason Coombs on Bugtraq