

Got Questions?



VERMONT COMPUTING INC.

Email us and we might feature your question in the newsletter!

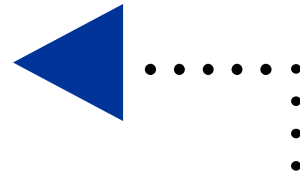
newsletter@vermontcomputing.com

Subscribe to this newsletter online! Visit:
<http://www.vermontcomputing.com/newsletter/>
or send an email to newsletter@vermontcomputing.com



Vermont Computing, Inc.
23 Merchants Row
Randolph, VT 05060
Tel: (802) 728-9217

Take one!



Store Hours: Mon – Fri 8:00 – 6:00 Sat & Sun 10:00 – 12:00

How to secure a hard drive from unwanted data retrieval



**Vol 7 Issue 9
May Part 1
Newsletter**

IN THIS ISSUE:

COMPUTER TALK:

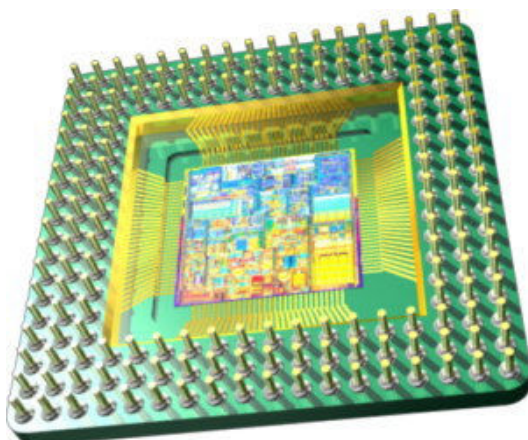
- *MS PATCH FIRES OFF 14 CRITICAL UPDATES*
- *NEW WORM TARGETS PORTABLE MEMORY DRIVES*

A BIT OF ADVICE:

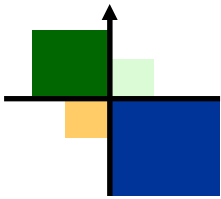
- *HOW TO REALLY ERASE A HARD DRIVE*

SHUTDOWN:

- *BEST EXCUSES IF YOU GET CAUGHT SLEEPING IN YOUR CUBICLE*



IBM Chip Uses Self-Assembling Material



COMPUTER TALK

MS Patch Tuesday (May 8th) Fires Off 14 Critical Updates

<http://www.extremetech.com/article2/0,1697,2127521,00.asp>

Microsoft has released patches for 19 vulnerabilities, 14 of which are critical, hitting at holes in Excel, Word, Office, Exchange, Internet Explorer, cryptographic technology and the whopper of them all, the zero-day vulnerability in the DNS Server's use of RPC....

An exploit for the DNS RPC (remote procedure call) interface vulnerability was discovered in the wild in April. Within a week of its discovery, four new malicious programs popped up, each trying to take over systems by prying open the DNS hole.

The DNS remote code execution vulnerability affects server-grade operating systems, including Windows 2000 and Windows Server 2003, and only those that have the DNS service enabled, such as Domain Controller, DNS Server or Microsoft Small Business Server configurations.

New Worm Targets Portable Memory Drives

<http://www.extremetech.com/article2/0,1697,2126656,00.asp>

Researchers from security vendor Sophos say a new worm targeting removable drives is an example of a potential security threat for businesses.

The SillyFD-AA worm searches for removable drives such as floppy disks and USB memory sticks and creates a hidden file called autorun.inf so that a copy of the worm runs the next time the device is connected to a computer running Windows. In addition, it changes the title of Internet Explorer windows to say that the computer has been "Hacked by 1BYTE."

In an interview with eWEEK, Graham Cluley, senior technology consultant at Sophos, said the worm has not been widely distributed, and that researchers were warning the public because of the potential danger. It would be easy, he continued, to add to the worm the ability to transmit through other routes, such as e-mail and instant messaging.

"It is interesting to see hackers using different techniques in their attempt to break into peoples' computers," said Cluley, in Abingdon, United Kingdom. "This type of attack is perhaps understandable as so many businesses these days do have e-mail gateway protection in place...they can scan files coming into their company via e-mail attachments, but can't check the files coming in attached to the keychain in peoples' pockets."

Sophos researchers said hackers are increasingly looking for ways to attack businesses that will meet less resistance than more traditional e-mail-borne viruses and malware. The

company's security experts advise users to disable the auto-run facility of Windows so removable devices do not automatically launch when they are attached to a computer. Any storage device that is attached to a computer should be checked for virus and other malware before use, Sophos officials said.

IBM Chip Uses Self-Assembling Material

<http://www.extremetech.com/article2/0,1697,2125510,00.asp>

SAN FRANCISCO - IBM has developed a way to make microchips run up to one-third faster or use 15 percent less power by using an exotic material that "self-assembles" in a similar way to a seashell or snowflake.

The computer services and technology company said the new process allows the wiring on a chip to be insulated with vacuum, replacing the glass-like substances used for decades but which have become less effective as chips steadily shrink.

It is the latest achievement for IBM researchers, who have announced a number of advances in recent months allowing chips to get smaller despite challenges posed by physical laws at those tiny dimensions....

The technique works by coating a silicon wafer with a layer of a special polymer that when baked, naturally forms trillions of uniformly tiny holes just 20 nanometers, or millionth of a millimeter, across...

"The problem they needed to solve was how to create lots of deep little wells in the insulation area between the wires," said Nathan Brookwood, who runs Insight 64, an industry consultancy.

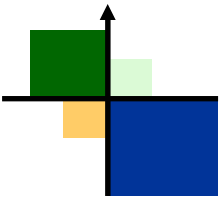
"Typically, whenever they tried, they ended up making a chip that was like Swiss cheese and had no mechanical integrity," Brookwood said.

Kelly said that while IBM plans to use the process in its chips in 2009, it has already made prototypes based on existing designs and it could employ the technique sooner.

IBM will also "selectively license" the technology to partners, Kelly said. IBM has research efforts with No. 2 computer processor maker Advanced Micro Devices Inc., Japan's Toshiba Corp., and others.

Last month, IBM said it had found a way to stack the components of a chip on top of each other, making them faster and more energy efficient by cutting the distance an electrical signal needs to travel.

In January, the company said it had solved a long-standing obstacle in drastically cutting electricity leakage in chips. That announcement-made alongside a similar but separate one by Intel Corp.-was hailed as the biggest advances in transistor technology in four decades.



A BIT OF ADVICE

How to REALLY erase a hard drive

<http://blogs.zdnet.com/storage/?p=129&tag=nl.e040>

You may already know that "deleting" a file does nothing of the sort. But did you know that your disk drive has a built-in system for the secure erasure of data? No? Then read on.

What do you mean "delete" doesn't delete?

File information is maintained in a directory so your operating system can find it. All that "delete" does is erase the file's reference information. Your OS can't find it, but the data is still there. That's what those "file recovery" programs look for: data in blocks that the directory says aren't in use.

If you keep business, medical, or personal financial information on disks, simple deletion isn't enough to protect the data when disposing of the equipment. Besides identity theft, data loss may leave you or your company liable under federal laws such as HIPAA, Sarbanes-Oxley, Graham-Leach-Bliley or other state laws. Criminal penalties include fines and prison terms up to 20 years. Not to mention the civil suits that can result.

So what's the magic?

Something called Secure Erase, a set of commands embedded in most ATA drives built since 2001. If this is so wonderful, why haven't you heard of it before? Because it's been disabled by most motherboard BIOSes. Secure Erase is a loaded gun aimed right at all your data. And Murphy's Law is still in force. But hey, if you're smart enough to read Storage Bits, you're smart enough to not play with Secure Erase until you need to.

How does Secure Erase work?

Secure Erase overwrites every single track on the hard drive. That includes the data on "bad blocks", the data left at the end of partly overwritten blocks, directories, everything. There is no data recovery from Secure Erase.

Says who?

The National Security Agency, for one. And the National Institute for Standards and Testing (NIST), who give it a higher security rating than external

block overwrite software that you'd have to buy...Secure Erase is approved for complying with the legal requirements noted above.

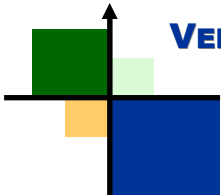
The University of California at San Diego hosts the Center for Magnetic Recording Research. Dr. Gordon Hughes of CMRR helped develop the Secure Erase standard. Download his Freeware Secure Erase Utility, read the ReadMe file and you're good to go. To use it you'll need to know how to create a DOS boot disk - in XP you can do it with the "Format" option after you right-click the floppy icon in My Computer.

Instructions for using HDDerase.exe

Copy the downloaded file, HDDerase.exe onto the created floppy/CD-ROM bootable DOS disk. Boot the computer in DOS using the bootable disk. Make sure to set the correct boot priority setting in the system BIOS. Type "hdderase" at system/DOS prompt to run HDDerase.exe. All ATA hard disk drives connected to the main system board will be identified and their information displayed. Make sure that the jumpers on the hard disk drives are correctly configured. Avoid setting the jumpers to CS (cable select) on the hard disk drives. Master or slave jumper setting is preferred. There's more, but if this is more than you want to deal with then Secure Erase isn't for you.

Can HDDerase.exe be used to erase my onboard SATA drive?

Yes, but some BIOS configuration may be required. Since hdderase.exe only detects drives on the primary and secondary IDE channels (P0, P1, S0, S1) the BIOS must be configured so that the SATA drive is detected one of these channels. This can be done by switching the SATA drive from "enhanced mode" to "compatibility mode" in BIOS (compatibility mode is sometimes called "native mode" or "IDE mode"). E.g. BIOS >> IDE configuration >> onboard IDE operate mode >> compatibility mode. Note - not all BIOSs support this feature.



SHUTDOWN

Sleeping on the job

Best excuses if you get caught sleeping in your cubicle:

<http://www.kissmyfloppy.com/pages/jokes.php?id=3&cat=all>

- It's okay...I'm still billing the client.
- They told me at the blood bank this might happen.
- This is just a 15 minute power-nap like they raved about in the last time management course you sent me to.
- I was working smarter, not harder.
- Whew! Guess I left the top off the liquid paper.
- I wasn't sleeping! I was meditating on the mission statement and envisioning a new paradigm!
- This is one of the seven habits of highly effective people!
- I was testing the keyboard for drool resistance.
- I'm in the management training program.
- I'm actually doing a "Stress Level Elimination Exercise Plan"(SLEEP) I learned at the last mandatory seminar you (boss) made me attend.
- This is in exchange for the six hours last night when I dreamed about work!
- I was doing a highly specific Yoga exercise to relieve work-related stress. Are you discriminatory towards people who practice Yoga?
- The coffee machine is broke....
- Someone must've put decaf in the wrong pot.
- Boy, that cold medicine I took last night just won't wear off!
- It worked well for Reagan, didn't it?
- I was cross-training for telecommuting. (Next, I watch the Walton's)
- Ah, the unique and unpredictable circadian rhythms of the workaholic!
- I wasn't sleeping. I was trying to pick up my contact lenses without using my hands.
- The mailman flipped out and took out a gun so I was playing dead to avoid getting shot.
- I thought you (boss) were gone for the day.