

McHenry County Computer Club

USERS GROUP FOR PC-COMPATIBLE SYSTEMS



SEPTEMBER 2008
VOLUME 25 No. 9

The **September 2008** meeting of the McHenry County Computer Club is **September 13**, at the Salvation Army Building, 290 W. Crystal Lake Ave., in Crystal Lake. Enter the building at the parking level double door under the awning. The treasurer will be there by 8:30 AM for Club financial transactions.

Membership

Our membership is \$26.00 a year. **NOTE:** This fee offsets the running of the club; membership benefits include help with computer problems. Please pay Lyle Giese, our treasurer, or the designated Board Member in his absence.

Meetings : 2nd Saturday of the month.

N.B.: The Salvation Army has asked us not park in front of the dumpsters or in other designated spaces. Your vehicle is subject to towing if it is not parked in the appropriate spaces.

Meeting Agenda

09:00 General Business Meeting
09:15 Demo: Helicopter - John K ; Vista Overview - Jim B
10:00 Break
10:15 Q&A
10:45 Anniversary Party

The Newsletter is published monthly by McHenry County Computer Club, online.

Editor-in-Chief: Lucë York

Direct inquiries, comments, articles to the Editor to Lucë at info@Mc3ComputerClub.org

Direct technical questions to MC3 at: info@Mc3ComputerClub.org

MC3 website: <http://www.mc3computerclub.org/>

UPCOMING DEMOS

September - Overview of Vista - Jim Bierle; Helicopter flying - John Katkus

October - Routers - Lyle

November - Excel - Jack

Remember that the September meeting is our 26th Anniversary celebration (*unless I have managed to miscalculate - Lucë*).

Your ISP's DNS server won't get a direct answer from the root servers. It will get a pointer to one that should know. It's possible to go through several of these referrals before it gets to the authoritative DNS server. Those are the servers that will have all the answers for the domain mc3computerclub.org in our example. At that point, they will get the proper IP address for www.mc3computerclub.org.

This process of asking around is called recursion. Your desktop computer is not capable of doing recursive queries without extra software. Not all DNS servers will accept queries that require recursion for you. For security reasons, the DNS servers at LCR Computer will not do recursion for anyone out on the Internet. LCR's servers will provide answers for the domains that it is authoritative for, however, like mc3computerclub.org or lcrcomputer.com.

The other factor is that all DNS data has a TTL field (Time To Live). Unless you are dealing with DNS for dynamic IP address space, the TTL is set to 1 or more days. So once a DNS server gets an answer, it won't ask again, but serves that cached data instead until the TTL expires for that data.

Where do the security issues come into play here? DNS servers use UDP (User Datagram Protocol) packets to communicate wherever possible. UDP is considered sessionless. The asking server sends a UDP packet and hopes the other server gets it and will respond.

The other method for data communication uses TCP (Transmission Control Protocol) packets. TCP packets are useful for transferring more data and when a session setup is required. In order to properly use TCP, three packets are used to set up the session and three packets are used to take the session down. That's six packets that do not contain any data that is useful to DNS. Plus at least two data packets.

So you can get the same data in two packets using UDP or use eight packets using TCP. That may not seem like much, but for very busy DNS servers it can mean the difference in handling the traffic or dropping the traffic because the amount of traffic will overwhelm the data path or the server itself.

But UDP packets are sent and the underlying application has to figure out if it gets a valid answer. Two methods are used to determine if the received data was real or fake in DNS servers. One, the data is sent from a high order port (greater than 1024), so we look for the data on that same port. The other is a transaction ID assigned and transmitted on the packet sent out.

Hackers attempt to hijack that communication by guessing the next port that will be used and what the next transaction ID will be. Because many DNS servers will do recursive lookups for you, it's easy to find servers that will go out and try to find data for you. Now comes the guessing game.

If the hacker guesses right to the port number and the transaction ID and his packet gets to the DNS server before the legit packet gets there, he won and the DNS server now holds the hackers data instead of the legit data. And because he is no dummy, he will put a very long TTL on that data to try to make the DNS server hold and use his data for a long time.

That's what happened in Dallas, TX. A DNS security firm discovered that they were going to a fake Google website. In turn, they traced it back to an AT&T DNS server for DSL customers in Texas that was holding bad data for Google. The bad guys won that battle of packets and poisoned the cache on that DNS server.

The problem is that many DNS servers were not programmed to use random enough port numbers and transaction IDs in their requests, and the bad guys had an easy time guessing the next working combination to hack against. Back in June, that was what the flurry of patches was about.

Someone figured out that there was a problem, and there was huge undertaking at several levels and across many companies to put out patches for DNS server software at the same time. They did a pretty good job of keeping it a secret until the patches were released.

But even now, those patches do not cover the issue 100%. It's estimated that hitting a server from two workstations with 1g connections, the bad guys could make a correct guess once in 10 hours. That's a lot of traffic and should get noticed.

There are more things in the works to make DNS more secure, but because of the nature of the Internet, it will take several years at least to implement these changes in software and then convince everyone to convert to the new system.

There is a website that will test the DNS servers your computer is using to see how random the port numbers and the transaction IDs are.

<https://www.dns-oarc.net/oarc/services/dnsentropy>

Click on the Test My DNS button and they will make some specific DNS queries from your computer via a java script and can send back two small graphs for each DNS server your computer is using.

One graph plots the source port numbers and the other plots the transaction IDs used. If there is a pattern to those numbers, the servers will get a less than great rating and you could visually see a pattern in the dots.

OpenDNS at <http://www.opendns.com> claims to have DNS servers that are immune to this problem. You can change the DNS servers used on your computer in the Network properties if you want. I am not going to go into how to do that here.

But more recent research would seem to indicate that OpenDNS's security may be good, but is probably not 100% immune. YMMV (Your Mileage May Vary.)

Contributed by Lyle Giese

Questions & Answers

Q: In Excel, is there a way to lock in the wrap text or do I have to keep selecting it for each cell?

A: Excel formatting can be applied to several cells at one time, even non-contiguous cells. Thus, if you have a number of cells to which you want to apply Wrap Text, select them and step through Format Cells, Alignment, Wrap Text, OK to apply the setting. Generally, the cells will expand to additional line(s) to show the wrapped text entry after you select OK. Depending on how the spreadsheet is set up at this point, you may have to adjust the column width, either up or down, to get the effect you want.

Alternatively, if you know you want to “wrap text” as you enter information in a particular area of a spreadsheet, you can set the format for that group of cells before starting data entry. The wrap text then is applied as you enter data in the cells. For example, if you are using column A as description for the cells to the right, set the width of column A to 30 characters (say) and apply Wrap Text to all of column A. Then, as you enter data in a cell in column A, the cell automatically expands to a second line if you enter data beyond 30 characters and to a third line if you go beyond 60 characters and so forth.

Q: When adding a USB card to a computer, is it necessary to have a driver to get it to function?

A: Sometimes, but not always. It depends on the function the card provides and the version of Windows you are running.

Q: Can I switch external CD burner software without removing the existing software first?

A: Sometimes. Usually it will work, but if the software has a systray applet that tries to auto-detect that you put in a blank CDR, that function could conflict with a similar applet in the new software.

Q: Can I dual boot an XP computer from a backup hard drive from Win98?

A: It's possible. It depends more on whether you have or can obtain Win98 drivers for the hardware in the computer. Remember Win98 is 10 years old and not supported any more. HP, for one, has pulled all Win98 printer drivers.

Q: Can I create a recovery CD from a computer more than once?

A: I am assuming that you are talking about where you are asked to create recovery CD's for a new computer. Usually that application will only run once. But there is no reason you could not create a copy of those CD's.

Q: Windows 2000 shuts off a short time after booting up. CHKDSK /r does not help. Safe Mode is ok.

A: 99% of the time this happens for one of two reasons. The system overheats and does a thermal shutdown. The other is that you have a UPS for your computer and set it up to turn off the computer when power goes out. If the UPS malfunctions or you took **the UPS off without** removing its software, it can turn off your computer.

Q: What is a good/best way to communicate to people in other countries (International/Australia) by phone or computer?

A: Email always works well and free email accounts can be obtained on several websites. Voice communications work fairly well with most recent instant messenger programs from Yahoo, AOL and Microsoft. Skype is another option for voice. Voice may not work well with dialup Internet service.

Q: Is it ok to install XP SP3?

A: There are a couple of gotcha's. I doubt they will 'go away'. Some companies installed WinXP from one image for both Intel and AMD CPU-based motherboards. SP3 does not like the extra files the Intel CPU's needed if they are found on an AMD computer.

If you have IE7 installed and then install SP3, you will not be able to remove IE7.

Q: Has anyone heard whether it is bad to run registry cleanup programs with third-party software?

A: Registry cleanup programs try to guess at what is not needed or is bad information and remove it from the registry. Most of them do a good job, but they do make mistakes.

I am not sure what is meant by third-party software here, but there are plenty of 'choices' out there for registry cleaner programs. Some of them are just plain bad or worse. You need to be careful when picking out a registry cleaner program.

Q: On shut down, instead of turning off, I get a message 'Safe to turn off computer.' Can this be switched to normal shut down?

A: It means WinXP cannot figure out how to turn off the computer for you. Something has been installed that interferes with the function or WinXP never could figure that out for you.

Q: What is OpenDNS?

A: OpenDNS is a service provided much the same way Yahoo or Google is provided to us. OpenDNS allows you to reset your computer's DNS to their servers to avoid DNS problems that have been the talk of the club and the Internet recently.

OpenDNS CLAIMS to not be vulnerable to the DNS technical issues that have come to light recently. But further technical explanations seem to indicate no DNS software is completely immune to those issues. [\[See article before Q&A section.\]](#)