



GET INFO

September 2003

1

Inside:

The Vulnerability of the Internet to Terrorists	1
Prez Sez	4
Up To Date	5
August TMUG Minutes	5
Reunion SIG Announcemnt.	6
OSX Desktop Trash Can	6
September Program	7
Summer Showcase Photos	7
Membership Form& Map	8

Programs:

This month:

OS X Networking / File Sharing Workshop

(See p.7 for future programs)

TimeTable:

- Deadline for Newsletter Copy/Photos: 9/29/03
- Officers' Meeting (open to all) 4th Monday of each month, 6:30 pm, Golden Corral on Highway 55
- Regular Meeting Schedule:
 - 6:30-6:45-Announcements
 - 6:45-7:40-Q&A, then Break
 - 7:45-8:40-Program
 - 8:40-8:45-Door Prize Drawing
 - 8:45-until-Off-Site"Networking" at Location to be announced

Email: editor@tmug.org

Apple, the Apple logo, the MacOS logo and Macintosh are trademarks of Apple Computers, Inc., registered in the U.S. and other countries.

The Vulnerability of the Internet to Terrorists

by Adam C. Engst <ace@tidbits.com>

With terror alert color codes coming and going, and the constant presence in the news of both terrorist activities and anti-terrorist efforts, it's hard not to wonder what the vulnerability of the Internet might be to terrorists. To answer that question, I turned to Chuck Goolsbee, Vice President of Technical Operations at the large Web hosting and server colocation firm digital.forest (where the servers that maintain much of our Internet presence have lived for years). Founded in 1994, digital.forest has all the large-scale data center amenities—redundant fiber, multiple backbone connections, redundant power, secure facility, and so on—but with the advantages of a small-scale ISP-friendly, knowledgeable tech support who understand multiple platforms, personal service, reasonable pricing, and more. digital.forest also is the oldest and largest Mac-savvy hosting and colocation facility, housing many well-known Macintosh Internet sites. And as vice president of technical operations, Chuck pays a lot of attention to anything that could cause interruptions in digital.forest's service. <<http://www.forest.net/>>

Adam: Chuck, is there any way terrorists could physically attack the Internet?

Chuck: In terms of physical locations go, there are so many places that "are" the Internet that attacking one, or even several at once, would have negligible overall affect to the entire network. My point here is that unlike 20 years ago, the Internet is no longer a bunch of interconnected wires. It is in many ways, everywhere.

That said, there are a handful of places where too much stuff is concentrated in one physical location. An inhabitant of the network operations lists I subscribe to, Sean Gorman, has written his dissertation documenting the Internet and other infrastructure items in the U.S. It represents the first ever complete "physical map" of much of the Internet, and now has been deemed a "security risk" by some government people who fear exactly what your question asks about. They see Sean's dissertation as a guide for attacking the Internet. <<http://www.washingtonpost.com/wp-dyn/articles/A23689-2003Jul7.html>>

The irony here is that everything Sean used to make his map is public information. Some of these places are even geek tourist spots! I'll admit that I have visited a few locations where transoceanic cables make landfall, and yes, my wife thought I was nuts when we drove out to Land's End in the UK to see what she properly interpreted as a "nondescript concrete box."

But to reiterate, any such physical attacks, even on important Internet connection points, would be devastating to the companies directly involved, but the Internet would, as the cliché says, route around the damage. Even if your packets had to travel three times the physical distance, they'd still find an interconnect point that would get them to their final destination.

Adam: So in the short term, traffic to specific Web sites might be cut off or at least slowed down by less efficient, but still functioning, routes?



TMUG OFFICERS

President

Smythe Richbourg (pres@tmug.org)
919-796-6705

Vice President

Chips Chapman (vp1@tmug.org)
336-226-7425

Treasurer

Jeff Cole (treasurer@tmug.org)
919-806-0109

Secretary

Frank Crigler (secretary@tmug.org)
919-530-1697

BBS System Operator

Paul Lemieux (plemieux@tmug.org)
919-460-0736

Vice President of Publicity

Bob Seila (vp2@tmug.org)
919-541-2214

Web Master

Phi Sanders (webmaster@tmug.org)

Newsletter Editors

Melanie Crain 919-489-8525
Kathy Mason 919-250-4170
(editor@tmug.org—goes to both editors)

All members are invited to the following:

Palm Computing Special Interest Group (Triangle Adherents of Palm Information Technology – TAPIT)

Meets on 3rd Mon. at Dakota Grill in Cary
Smythe Richbourg (palmnews@tmug.org)
<http://tapit.interpug.com> (map on page 7)

– and –

Digital Photography Special Interest Group

Meets on 1st Mon. at Smythe's office (see
map and weblink on page 6)
summer contact person: Lewis Midyette
(midyette@nc.rr.com) 919-785-7185

TMUG Hotline 919-833-8501

TMUG Website www.tmug.org

Chuck: Yes. The Internet is not a single network, it is many networks, all interconnected, usually at multiple points. The obvious attack targets are major exchange points where many of these networks meet. Our local one here in Seattle is a building downtown called the Westin Building (if I recall correctly, it is the former headquarters of the Westin hotel chain).

<<http://www.westinbuilding.com/>>

Virtually every major Internet provider has some or all of their Pacific Northwest presence there. It makes economic sense to "meet" in a single location, but if you are thinking in defensive terms, it is a weakness. Through some luck and a little planning, only half of digital.forest's upstream bandwidth comes directly through that building (via a Gigabit Ethernet connection); the other half comes in via an OC-12/SONET ring from Verizon. The latter originates in Everett, WA, mostly due to our location northeast of Seattle. So even if the Westin Building were damaged, we would have connectivity from alternate sources. In larger terms the whole Internet works like this, with multiple paths to most destinations. The routing protocols that manage the Internet's traffic constantly update and change the pathways for data, so that when a route disappears, alternatives are ready and traffic still flows. But honestly, I fear a large scale natural disaster, such as the earthquake that struck Kobe, Japan, more than I do a terrorist attack.

Adam: And how long would it take for more-or-less normal operations to start up again?

Chuck: That would of course depend on the nature and scale of the incident. Some operations could be up in just hours, and some could take weeks. A major earthquake could cause widespread damage that would make rebuilding that much harder. But since we're talking about terrorist acts, the September 11th events serve as a good example. The attack in New York caused significant damage to major telecommunications facilities in lower Manhattan. Some services were disrupted for a few hours, most were out for a period of several days, and a few required weeks to replace or repair fully. The services on which people depend for critical communications, such as standard dial tone and 911 emergency services were the first to be restored. Email and Web traffic were (justifiably) further down the list. In this case, the impact was highly localized, being confined to an area immediately surrounding the World Trade Center.

Adam: It doesn't sound like a physical attack would do much to the Internet. What about terrorists releasing worms? What effect might that have?

Chuck: Take two examples, MSBlaster and SoBig.F, which were targeted at specific weaknesses in Microsoft Windows's RPC and Outlook, respectively. The damage they caused as they spread was basically a denial of service (DoS). MSBlaster was easily defeated by Microsoft as they removed the target of the planned DoS attack. SoBig.F's ultimate purpose is not yet known. What the press thought was the attack was really just the spread... the massive amount of traffic caused as these worms propagated through the Windows machines connected to the Internet. No specific damage happened other than to networks that were completely unprepared. However, if core functionality such as DNS was disrupted in a serious manner, the damage would be global in scale. Without DNS the Internet loses its human-readable nature. I may know that 216.168.37.138 is www.forest.net but very few other people do; DNS does the necessary lookups behind the scenes.

Also, those sorts of worms and viruses usually don't have a political agenda behind them, beyond pointing out the flaws in running code. I can't see them meeting the goals of a terrorist organization—even if the worm displayed some sort of political message, it would exist only for a relatively short time until the anti-virus software and firewalls were updated.

Adam: Let's focus on DNS then. How hard would it be to bring down DNS?

Chuck: Very difficult, because DNS is a resilient system that was designed from

the start to be massively distributed. Also, one of the frustrations of dealing with DNS is propagation time, the time it takes for changes made to DNS to become usable across the whole Internet. That built-in delay makes attacking the DNS system as a whole extremely difficult.

Adam: But as much as DNS is distributed, aren't there root servers that are more important than any ISP's DNS servers?

Chuck: Yes, DNS does have a weakness in that all DNS servers defer to a system of root servers that ultimately control which lower-level DNS servers have authority over which domain names. Last I checked there are 13 root servers distributed around the world in obvious high traffic Internet exchange locations. The organization that oversees their operation has made efforts to secure them by making their operating systems and DNS software be more diverse, and therefore less susceptible to attack. They have also built mirrors and clones of root servers in physically diverse locations. There have been distributed denial of service attacks made on the root servers, but to my knowledge these attacks have usually been stopped before they can do any real damage. A successful attack on the root servers would be very difficult to achieve, but significant in its effects.

<<http://root-servers.org/>>

Adam: Interesting—running multiple operating systems increases the overall resiliency of the system, since most attacks are specific to an operating system or will affect different operating systems differently.

Chuck: Precisely. The DNS system and others like it are resilient, but I think that's mostly due to the nature of the people who operate them. These are, for the most part, smart and resourceful folks. Systems, when they are virtual in nature, can usually be reconstructed swiftly when interrupted—there are always multiple backups. Think about it, even a worst-case scenario: if every DNS root server were destroyed, they would likely be replaced and operational within a reasonable amount of time. It might be days, or even a week or two at most, but that's it.

Adam: What about denial of service attacks—could terrorists use them successfully? I remember some a few years ago that caused significant problems for Yahoo and a few other major Internet companies for a while. And distributed denial of service attacks wouldn't require nearly the same level of knowledge as attacking root servers.

Chuck: Remember that DoS attacks are basically noise--high volumes of traffic directed at a target to overwhelm it, or its network connection, thus rendering it unusable or unavailable. It is relatively easy, trivial even, to bring down even a major site temporarily with a DoS attack. However they are also difficult to sustain for long periods of time because network operators (those smart and resourceful people I mentioned) have built and continue to maintain loose, but well connected communication networks. These human networks cooperate to identify and stop DoS

attacks. DoS attacks are ugly and frustrating, and just about all of us who run networks have experienced them firsthand, so we do our best to stop them when we can. One of the current worries in the operational community is that SoBig.F is really designed to turn infected Windows machines into zombies for carrying out distributed denial of service attacks (which originate from many machines all at once and are more difficult to combat than normal denial of service attacks). But to answer your question: Sure a terrorist could DoS somebody, but a DoS attack is probably not the sort of highly visual, news-making media event that terrorists use. It is devastating to the victim, but invisible to everyone else.

Adam: Let's go back to this concept of resilient systems. Is a highly resilient system thus 100 percent reliable?

Chuck: No, not at all. Internet users have to understand that the Internet's resiliency stems from its distributed and complex interconnected nature. These sort of systems are never 100 percent reliable. They are not designed to be. They are designed to continue to function while parts are not working. One of my favorite quotes comes from a network operator named Sean Donelan, who said, "Murphy's revenge: The more reliable you make a system, the longer it will take you to figure out what's wrong when it breaks." It's funny because it's true, resilient systems can still function even when "broken."

Even the September 11th attacks, which caused the complete disruption of air travel for a few days, couldn't really stop air travel completely. The system adapted and continued. Security screening is more stringent, some airlines and aerospace related businesses are still feeling the effects, but we consumers can still fly.

So even if there were some attack that successfully targeted some core system of the Internet, it could not stop it for very long. Some companies doing business on the Internet would suffer, and users would probably be confused and irritated for a while, but overall the incident would just be that, an incident.

Adam: But many people have become accustomed to the Internet just working all the time.

Chuck: Indeed. I work in the uptime business. I know that our clients fully expect 24/7 uptime so their Web sites and email servers are always online. We had an outage in March of 2003 that lasted 55 minutes. It was the most agonizing 55 minutes of my life, and many of our clients were furious about it. It was the first serious unplanned outage we had experienced in over four years, but it still cost us much in terms of money and credibility with our clients. In the aftermath we have made many changes, technical, staffing, and procedural, based on lessons learned. I have spoken with many clients and appreciate why they require that uptime.

The hardest part of my job is explaining to clients the definition of uptime. Frequently the issue is something that we have no control over, like a fiber cut in Utah that forces packets through Dallas instead of Chicago. People assume

that "It is the Internet, it is always *_on_*, right?" The reality is that parts of it are always *_off_* at any given moment of every day, and that while the Internet will route around damage, the result is that it may take a while, or things may not work as they did even a few moments ago.

Adam: Okay, but let's take the other point of view. How important is uninterrupted Internet accessibility? I'm talking about life and death stuff here, not just someone being unable to check headlines on CNN or have customers come to a Web site.

Chuck: Much as it may not seem like it sometimes, uninterrupted Internet accessibility is not really a matter of life and death. Like other accoutrements of modern life—televisions, telephones, and so on—the Internet is not something that is required to sustain life, no matter what some geeks may think. Yes, it has economic and social value, but it is not, as far as I know, required to maintain life. So while damage that occurs from an attack on the Internet can have real financial and even emotional effects, it's important to maintain a sense of perspective.

Adam: From what you're saying, it doesn't seem as though the Internet makes a particularly attractive terrorist target.

Chuck: I guess that depends on the nature of the Internet as a target. The September 11th attacks were aimed at targets with high visibility and symbolic representations of U.S. economic and government power. I have a hard time thinking of the Internet in those terms. The Internet is really more of an infrastructure item than a symbolic one, and terror's goal is visibility. Infrastructure becomes a target when nation-states are at war with one another; terror does not usually fall within that definition. Bruce Schneier made this point well in an editorial a few months ago.

<http://www.counterpane.com/crypto-gram-0306.html#1>

Adam: What about defacement of Web sites? Would it be a problem if the White House Web site, or other high profile sites like Yahoo, Amazon, and eBay, were attacked and used to disseminate political propaganda?

Chuck: Web site defacement is basically digital graffiti. It can be an embarrassment, but it doesn't have any operational impact on how packets move around the network. I also believe the Internet is a secondary news source, meaning I doubt that most people use it as their only source of news, especially news of their government. Defacing, or changing the content of all media; newspaper, TV, radio, Web sites, etc., borders on the impossible. Web site defacement is more of a prank than a terrorist threat.

Adam: So in the end, from the perspective of Internet users, the worst the Internet is likely to suffer at the hands of terrorists would be a major inconvenience attack. That's overly glib, of course, since a physical attack could result in casualties, and even these inconvenience attacks cost money to stop. Nonetheless, Chuck, thanks for enlightening us about this situation.

PayBITS: If Chuck's interview helped put your mind at

ease, contribute to TidBITS so we can bring you great interviews.

<http://www.tidbits.com/about/support/contributors.html>

Read more about PayBITS:

<http://www.tidbits.com/paybits/>

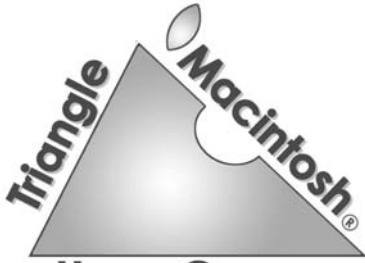
For information: how to subscribe, where to find back issues, and more, email info@tidbits.com. TidBITS ISSN 1090-7017. Send comments and editorial submissions to: editors@tidbits.com Back issues available at: <http://www.tidbits.com/tb-issues/> And: <ftp://ftp.tidbits.com/issues/> Full text searching available at: <http://www.tidbits.com/search/>

Prez Sez—Networks as Plumbing

No one likes to think about plumbing (unless you're a plumber!). It's one of those things that goes into the building, does it's business of bringing you what you ask for and dispatching what you want to send out, and stays out of the way. The only time it's the focus of attention is when it's not performing as expected. Have you ever lived in a house or apartment with inadequate plumbing? You're in the shower, and the water turns to an icy shock when the person in the room upstairs flushes the toilet or starts the dishwasher. Or, if the supply line to the building is too small, and several folks try to each get ready for their 8 AM class at the same time—once you have four or five showers running simultaneously, the water pressure drops to a trickle. I spent a year in an apartment building of eight units that shared a quarter-inch house line to the water main. I quickly learned to shower at times other people weren't thinking about it, in order to have that line all to myself.

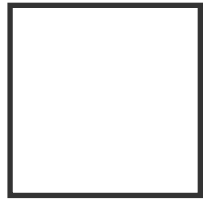
Networks are a lot like that—when they're working properly, they're behind the scenes, but when they're poorly designed or not adequate for your needs, they make themselves front-burner issues in a hurry. I was recently on the campus of a new school where 50+ students were frustrated in their attempt to download and install a simple software update. They all had new computers, the room was brand-new, and the servers belong to a large company that has MUCH more bandwidth than what we were trying to use. What was the problem? One of the administrators finally solved the issue—there was only a single 802.11b hub in the ceiling above the lecture hall, so only 11 active connections could be maintained! In the name of saving money, they had made the network unusable for the number of people the room was designed to accommodate.

When you got your first Mac and hooked it to a modem, things were dandy. You'd hop online, grab those three emails that had piled up over the two days since you last checked it, and log off. You kept up with your minutes online, because you were charged by the minute. Soon, you may have started to spend some time with that WWW thing, and spent a little more time online to read news stories or do a bit of research. Your service provider may have offered an "all-you-can-eat" package of unlimited



Users Group

P.O. Box 14724
Durham, NC 27709-4724

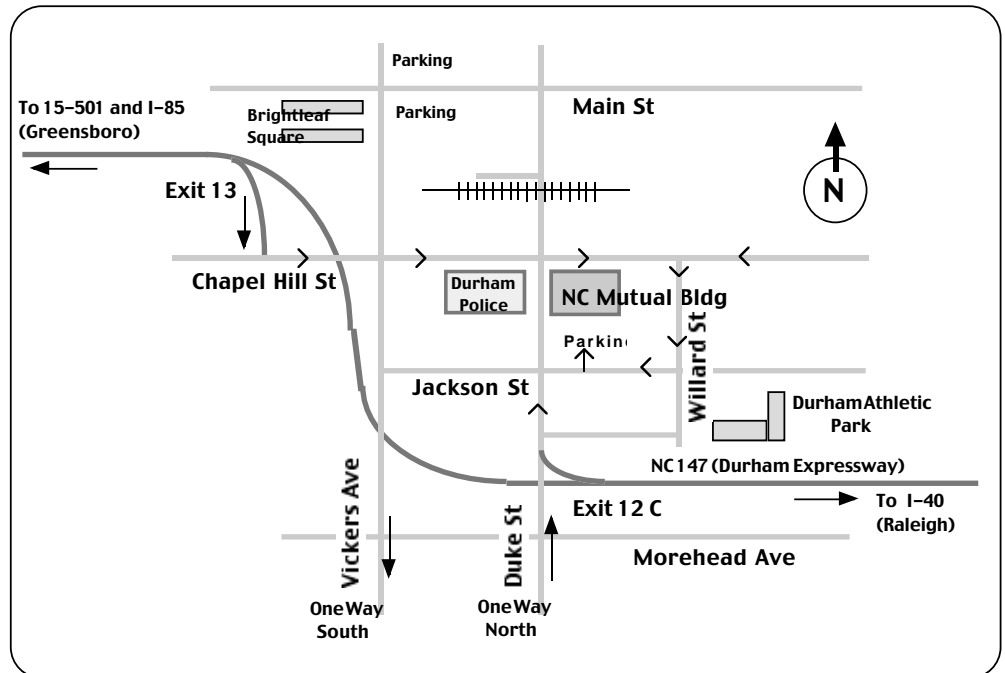


first class
mail

Meeting Location:

We meet the second Monday of each month at 6:30 pm in the Auditorium of the NC Mutual Life building in Durham, NC.

From I-40--Raleigh/RTP area: Take 147 (Durham Freeway) to Duke Street. Turn right onto Duke St., go to the first light, Jackson Street. The building is on the right across the street. Turn right onto Jackson, then immediately turn left into the lot and park.
When you get there: Go down the stairs to the right, not up the stairs. There is a guard at the entrance. Auditorium is on the right just off the lobby.



TRIANGLE MACINTOSH USERS GROUP

Membership Application

Membership

Renewal

Name: _____
Street: _____
Phone: _____
Business (if applicable): _____
City/State/ZIP: _____
Email: _____

Membership dues are \$35/year.

Make check payable to TMUG and send to:

TMUG - P.O. Box 14724 - Durham, NC 27709-4724