;login:

THE MAGAZINE OF USENIX & SAGE

April 2003 • volume 28 • number 2

inside:

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

motd

by Rob Kolstad

Rob Kolstad is currently Executive Director of SAGE, the System Administrators Guild. Rob has edited *;login:* for over ten years.

kolstad@sage.org

I have some comments on some of the recent press reports about “Cyber Terrorism” and computer security in general that contain fabulous quotes that the media has widely disseminated.

James A. Lewis, a Center for Strategic & International Studies analyst wrote a monologue entitled, “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats”[1]. Simply, he said:

> The assumption of vulnerability is wrong.

and in the paper’s stated context, he’s right. Its second paragraph defines: “Cyber-terrorism is ‘the use of computer network tools to shutdown critical national infrastuctures (such as energy transportation, government operations) or to coerce or intimidate a government or civilian population.” OK. It’s fair to define terms and then analyze the results of that definition.

The Gartner Group published a Q/A column[2] entitled *Cyberattacks and Cyberterrorism: What Private Business Must Know*. Here’s a quote that I think would be warmly received by those trying to decrease IT security budgets:

> Criminal cyberattacks are real and occur daily, while cyberterrorism is still a theory. Despite the hype, there is no known case of cyberterrorism. Government efforts focus on helping enterprises help themselves, and each other.

and, later:

> [The] Federal Bureau of Investigation defines terrorism as “unlawful or threatened use of force or violence . . . against persons or property to intimidate or force a government [or] civilian population [to further] political or social objectives.” GartnerG2 defines cyberterrorism as “terrorism attacks using a digital channel.”

Defining words is important. I think that defining words carefully and then using them publicly in quotes like “Cyberterrorism is still a theory” advances ideas that are counterproductive and can easily lead to decision-making with wide-ranging negative repercussions.

The recent Slammer Worm, 376 bytes of code that flashed through the internet recently, demonstrates one dimension of the state of the “cracking” art. The CAIDA folks have published an analysis called “The Spread of the Sapphire/Slammer Worm,” principally authored by David Moore. It contains these facts:

- The number of infected systems doubled every 8.5 seconds during its first minute. That’s 133x growth in a single minute.
- **At its peak (3 minutes in), it scanned 55,000,000 systems/second** (that’s a rate of 3.3 billion per hour). After that, no more network bandwidth was available. This is 100x the speed of the July 19, 2001 Code Red Worm, which hit 359,000 hosts.
- Of all systems possible to infect, 90% were infected within 10 minutes of the worm’s launch.
- The worm began to infect hosts around 05:30 UTC on Saturday, January 25, 2003 and exploited a buffer overflow discovered in July, 2002. A patch was released shortly thereafter, months before the worm was launched.
- 75,000 total hosts were infected.
- **A “better” vulnerability would have enabled infection of the entire internet in 15 minutes**, a “flash worm” or a “Warhol Worm.”
- Neither Code Red nor Slammer had a malicious payload.

Now, this sort of result doesn’t agree with Joshua Green comments for *Washington Monthly* in November of 2002[3]:

> There’s just one problem: There is no such thing as cyberterrorism – no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. . . . What’s more, outside of a Tom Clancy novel, computer security specialists believe it is virtually impossible to use the Internet to inflict death on a large scale, . . .

Dorothy Denning, Georgetown University Professor and cybersecurity experts says, “Not only does [cyberterrorism] not rank alongside chemical, biological, or nuclear weapons, but it is not anywhere near as serious as other potential physical threats like car bombs or suicide bombers.”

The article goes on to cite US$15 billion lost last year to various cyber attacks.

I believe that all these authors are writing words that are true: No one (hardly anyone?) has died from a computer attack, at least directly. The Slammer worm did infect some 911 computers; it’s not apparent that any real problems emerged from that.

But I think that all these analyses are missing the point. By demonstration, the computer and networking infrastructure is vulnerable. Slammer was a small worm with a relatively low success rate.

The networking infrastructure drives huge parts of the USA and world economies. It's easy to see that the fallout from the 9/11 attacks has contributed to the bankruptcy of airlines and, I believe, contributed to the lengthening of the USA economic recession. The attacks and their media coverage have moved USA society, at least, to a state of paranoia and fear not seen since the nuclear bomb scares of the late 1950s and early 1960s.

Please join me in a mental exercise about cyberattacks. Imagine that:

- a cyberattack causes the banking system to fail in its interbank money transfers.
- a cyberattack infects enough routers on the internet that traffic is slowed by 100x for weeks as the routers ping-pong infect one another.
- a cyberattack infects so many business computers that deliveries of commercial good of all kinds (including food) are halted for a week and then restarted manually with concomitant inefficiencies and lower throughput.
- a cyberattack takes out the airline reservation system, causing airlines to suspend their operations.
- a cyberattack takes out the computer control of the communications infrastructure, thus reducing telephone and other bandwidth by 100x and disabling long-distance phone calls, internet connectivity, and 80% of television programming relays

While none of these results would result in widespread death, any one of them would foment panic, chaos, and a deep new fear about the stability of at least the USA economic foundations and maybe its society in general. This level of disruption has the potential to destroy huge portions of the commercial infrastructure and unemploy millions of workers. It is easy to believe that the results would dwarf the depression of 1929.

Let's take a rational and calm course in "selling" computer security. Let's not use "Fear, Uncertainty, and Doubt" to motivate decision-makers. But please: let's not stick our heads in the sand, either. The Slammer Worm is only the latest realized threat. It is difficult to believe that no more threats exist. Keep your systems patched; heed vendors' warnings about upgrades; use common sense security precautions when designing and procuring software. Let's not make attackers' goals easier to achieve.

1. *http://www.csis.org/tech/0211_lewis.pdf*

2. *http://www.gartnerg2.com/qa/qa-0902-0091.asp*

3. *http://www.washingtonmonthly.com/features/2001/0211.green.html*