

Overcoming the Internet

Overcoming the Internet

What do you do with the modern problems of the Internet? Security and service attacks are common news items. Network load and bandwidth are real issues. Spamsters, snoopers, and crackers appear to be forcing companies to redirect development to building protective walls around themselves. In fact, the network landscape appears more and more like medieval castles or the lawless Wild West.

Companies are demanding security, and the dollars they are spending on firewalls, portals, single sign-on, etc., is mounting in the 100s of millions to billions of dollars. The problem is that the software only patches the inherent problems. *Inherent problems?* Yes, the problems that netizens are facing are primarily due to the nature of the Internet.

A Little History

Back when I first began working on and administering a few servers around 1985 at Brigham Young University, the network constituted several different networks linked in various ways through gateways. These gateways provided hopping points to get into BitNet, ARPAnet, etc. Our servers were part of the Internet itself. At that time, the Internet primarily harbored research and educational facilities as well as the U.S. Department of Defense. That all changed with the commercialization of the Internet.

Now, the various networks have either merged with or given way to the Internet simplifying transactions considerably. For example, sending an email message from the Internet to a destination on the BitNet, required using special routing sequences along with BitNet's own addressing scheme. Now, nearly all foreign networks recognize or are able to work with the name@company.network style of addressing. The migration from these disparate networks and protocols to a unified program has revolutionized the world.

The information revolution is due primarily due to the Internet, and the purpose of the Internet is to provide a dynamic and adaptive way for messages to get through. The routers, hosts and packets are mostly independent of each other making it very flexible and powerful: if one segment or route drops, the routers adapt and find new paths for the message traffic. The commercialization of the Internet increased this adaptability manifold. The evolution has been a tremendous boon to the flow of information: even peoples who are under more restrictive governments are gaining from the new, free flow of information.

Again, the strengths and plusses of new technologies bring downsides. The Internet moves messages from one place to another. No one checks the validity of the message or checks the originator. In fact, the message packets could easily be recorded and then replayed at any time or from any location. The nature of the Internet is its own stumblingblock.

The Problems with the Internet

The sheer power of the Internet is its capability to adapt. Also, since it has a lot of public pathways, the cost of connection is very cheap. At the same time, this power and decentralized ownership has led to the Wild West days. The challenges you face as a network expert include

Overcoming the Internet

security attacks, flooding, network load, and rising corporate costs. All challenges except for the corporate costs are technical in nature. This means that you can typically address them with a technical solution... well, most of the time.

The first challenge is a very serious threat to everyone on the Net: security attacks. The potential of taking an entire corporation down is very real -- something that has not been a possibility until recently. One insurance company estimated that if its network services were to fall to an attack, it would cost the company about \$10 billion in lost sales and lost trust.

One of the difficulties in tracking any network perpetrator is due to the Internet Protocol's message passing. The Internet can handle routing of traffic quickly and dynamically. In order to do this, you would have to ignore where the message came from and focus merely on the destination. This means that the message may be coming from a location non grata like a cracker or a spamster. Sure, some organizations (like the United State's FBI and CIA) actually track and record the messages for analysis, but those logs are typically unavailable to corporations worldwide.

Another difficulty is found in the hosting operating systems and services. Network-enabled operating systems are very complex; those with several program services (like email, HTTP servers, etc., leave a lot of openings for crackers to attack. Unless an operating system or service has security as its foundational design, it will never be secure.

An attacker also may not really be interested in getting into a site, instead he/she may simply want to take the site down. The tools the attacker may use are flooding, email spam, and viruses. All of these are because of the anonymous user. Anonymity is an expected feature of the Internet; however, in the hands of a prankster or malcontent, it can do almost the same amount of damage to a company as a network cracker. In almost all cases these three challenges reduces the availability of services, network bandwidth, and employee productivity.

Flooding a site essentially forces the site to pay the majority of its attention to the attacker while starving all the legitimate connection requests. It does not matter that you have the fastest servers on the planet. It's like having all the horsepower to beat everyone on the track but finding that you're burning more rubber than actually accelerating.

Spam (unsolicited email) is a real hidden cost. Most people that email spam know that they don't have to pay anything -- the reader does (in connection time and wasted labor). The US has a strange law that actually appears to protect spamming. As long as the spam includes a way to get off the list, the message is legal. Still, everyone knows that if you reply to the message, you may be removed from one list yet placed on another. Also, most email destinations (for removal) often don't really exist or are full and won't accept more messages.

The Net is very burdened with the weight of unsolicited email. Many home users get anywhere from 1-2 spam messages for every legitimate message. The time people spend trying to filter out the unwanted messages is relatively high.

Users also spend a lot of time avoiding, detecting, and removing viruses. The threat of computer viruses has growth its own industry: virus protection, detection, and removal. Companies like McAfee or Norton do a great job of protecting computers. However, their industry is

Overcoming the Internet

manufactured: without viruses, they would not be needed. Most large companies include some virus detection in the distribution of all their computers.

[network load]

Another challenge the network administrator may face is the increasing load on the company's network backbone. Professional technology tracking companies, like Gartner Group or META, warn their clients that if the network is moving towards support for Voice/Video over IP (VoIP), the technology may pass them by.

Intranets (company-owned networks) are not the only ones that are suffering. The Internet is increasing the bandwidth but not at the same rate as the demand. The demand for information has pushed the technology beyond its limit, and the demand has yet to level off. Again the cause is from the nature of the Internet: the user gains the perception that he/she solely owns the network segments from the computer to the host-server. In reality, the connection is shared between hundreds to millions of requests.

It is interesting to watch individuals try out simple tools like Microsoft NetMeeting with voice and video. They are surprised that the streams sometimes do not synchronize or that there is a time lag. They believe that the connection should be like a telephone. While expectations are higher than what the technology can currently offer, the upgrade costs keep the movement carefully slow.

[ROI/rising corporate costs]

Corporations are starting to look at the bottom line, especially with the current unsteadiness of the market. Costs are a significant issue for companies that now have to justify spending millions on Internet connectivity.

You've heard the claxons: *If you don't get on the Internet, you will be following not leading the future market.* A lot of companies have stepped to the plate only to find that the expected fastball of success has been more like a curve.

Companies often have a central Information Technology group that handles the day-to-day infrastructure maintenance. Services like networks, firewalls, servers, mainframes, databases, etc., all cost money, and the IT department often manages those costs, materials, resources, and personnel. Then, IT charges back the services to the requesting groups. No money really changes hands, it's all within the company, and some professional have termed it *funny money*.

Well, the internal clients are not finding it funny anymore. Some monthly costs range from \$200-500/month per connection. With functioning computers costing as little as \$1100 each, organizations are now considering alternatives.

The alternatives are as surprising as no connectivity at all. For example, many clients have found that their users really don't use the file sharing available on the network, and the Internet is not a requirement for many people's jobs. The only capability the users need is a printer. So, some groups are basically telling IT: "We're buying about 4,000 computers at \$750/ea, and don't worry, we'll take care of them ourselves." At \$200/month for IT support, the group can recover all the costs in less than six months!

Overcoming the Internet

Solutions and Potential Technical Directions

The Internet has introduced us to a full range of possibilities. The response has ranged from: “Charge!” to “Retreat!” The issues mentioned above are daunting, but you are likely to see some interesting changes in the near future.

As noted above, the rising costs of connection has forced some groups and companies to pull the Internet plug. The costs and risks are too high. Where is the return on investment? Really, the Internet is a venue (and mobile computing, i.e., wireless, is more of the same). If you don't really have a product without the Internet, you're in for a very rough ride. Likewise, if the job does not require connectivity, some companies are beginning to opt out of the Internet for now.

Similarly, some groups look at security from a balanced cost perspective: The cost of recovery vs. cost of prevention makes vulnerability appear cheap. This is a strange viewpoint, but it has some bottom line benefits. If they *don't* get hit during a year, they have saved all the costs of prevention. Likewise, if they *do* get hit, the likely impact may mean 1-3 days of recovery. This may equate to the costs of prevention (depending on the nature of the data and the size of the organization, of course).

Computer professionals frown on the thought of less security. However, under the light of profits, the option is still there, and some are moving towards it. Spam, flooding, and viruses fall into this light. The companies may standardize on a single virus detection but make no efforts to combat spam, even though it may take time away from employees' productivity.

The industry may solve flooding in one of two ways. The first way is to require connecting sites and ISPs to monitor their clients' usage. If the client does not comply by strict rules of conduct, the ISP would cut off his/her activity. You can also expect to see more site blacklisting. The reason is simple, if Internet companies cannot guarantee more security and profitability, we may see anonymity disappear.

The real way to solve the problems with Internet is to require complete source identification. Anyone person on the Internet, under these rules, must provide full identification for every transaction. This solution flies in the face of much of the Internet. However, it may be the final result.