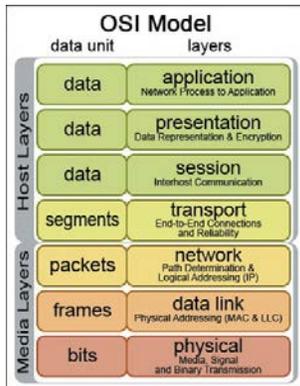


The Internet's Vulnerabilities Are Built Into Its Infrastructure

November 2009

By Paul A. Strassmann



Attackers concentrate on switches and routers when they strike at the network.

Protection of the Global Information Grid now has evolved into global asymmetric warfare. Engaging in this combat is the principal mission of the U.S. Cyber Command because the infrastructure of the Internet is fundamentally insecure, and the U.S. Defense Department depends increasingly on this cyber highway to function.

There are tens of thousands of defenders of the Internet infrastructure who must be vigilant around the clock, everywhere. Meanwhile, small teams of attackers can strike undetected whenever they choose, from wherever they may be in the world. This is why the contests between the defenders and the aggressors meet the definition of asymmetric warfare in its extreme form.

The reasons for the intrinsic vulnerability of the Internet can be found in the engineering of its switches, routers and network connections, which are owned by the Internet Service Providers (ISPs) and by the communication carriers. These flaws are pervasive. They were embedded 40 years ago when Internet protocols (IPs) were conceived.

Attacks from software bugs and computer viruses target computer devices such as servers, firewalls, desktops, laptops and smart phones. The government owns many such devices. Attacks include gaining unauthorized access, denial of service, malicious code insertion or password cracking. Hackers and other cyber criminals employ the Internet as a delivery means. Such attacks have a limited scope and therefore are seen as carrying geographically containable security risks.

More serious vulnerabilities can result from malfunctions in the Internet infrastructure. This includes connections to ISPs via points of presence, or POPs. They also include local area networks (LANs), wide area networks (WANs) and the switches that aggregate traffic. Malfunctions could occur in the high bandwidth infrastructure for traffic between the ISPs and network access point (NAPs). This includes the backbone interconnections among the NAPs. Therefore, the attack scenarios on the Internet infrastructure concentrate on its switches and routers.

Internet switches are intelligent network components with a wide-ranging set of software-defined services. These services are remotely maintained and upgraded in real time. They also generate remote diagnostics for control locations, which is one of their weak links.

The datalink layer is next to the bottom of the open systems interconnection (OSI) model. It suffers from gaping holes that can be exploited. The usual attack consists of altering the manufacturer's code in the switches. A number of major attack categories exist.

The open systems interconnection model layered approach, shown in this table, allows each subordinate, interdependent layer to provide services to the next higher layer as transactions are converted from lower to higher abstraction levels. Each layer, sending messages as binary bits, is interdependent; if a layer is compromised, the other layers will not know, causing Global Information Grid communications to cease.

Flooding attacks use tools that can generate more than 100,000 bogus entries per minute. This tactic overloads the switch so that it malfunctions.

Address resolution spoofing allows an attacker to sniff the data flowing to a LAN. The traffic either is modified or a denial-of-service condition is created.

The man-in-the-middle attack adds a third-party destination without the legitimate recipients being aware. The third party can extract passwords and confidential data. During a denial-of-service attack, the switch will not deliver packets and will time out, stopping all traffic.

The switch hijacking attack injects illegitimate connections that will pretend to be authentic. The added connections will take over control without the recipients being aware.

The spanning tree attack allows the inclusion of spare links as backup paths. Communications are then rerouted.

In a root claim attack, bogus bridge protocols are used to designate the attacker's station as the new root bridge. Once in control, a variety of malicious attacks can be launched.

The forcing eternal root election attack makes the network unstable by tampering with the routing algorithm to keep searching for the root switch, without ever finding it.

Another tactic is the virtual LAN, or VLAN, hopping attack. Subdivision into different LANs will be compromised if an attacker manages to send messages to the wrong links. When LANs support separately the Non-secure Internet Protocol Router Network and the Secret Internet Protocol Router Network, one of them can be used to initiate a denial-of-service attack on the other.

Routers are another major point of vulnerability on the Internet. ISPs and NAPs are connected through intermediate network devices known as routers. A router is a special-purpose, dedicated computer that makes connections when it receives a transmission from one of its incoming links, makes a routing decision and forwards the packet to one of its outgoing links. The routing decision is made based on the current state of the connecting links, as well as on the priorities that have been assigned to the various links in order to make selection of the next connection efficient. Each router uses a routing table to keep track of the path taken to the next network destination. Consequently, routing tables will never remain static but will change dynamically as conditions change in real time.

The management of routing tables must be automated for instant adaptation and for assuming additional functions, such as performing security operations in which reverse path verification is feasible. In this technique, the router looks up the source address of a message. If no route back to the source address exists, the packet is assumed to be malformed or involved in a network attack, and is dropped.

When a router receives an incoming packet, it passes it to the next router, defined as a "hop" to which the packet should be forwarded. The next router then repeats this process, and so on until the packet reaches its final destination. While the packets travel, they are vulnerable if an attacker is able to tamper with the router's software.

To attack routers requires information on how the network is configured and where the routers are located. One approach is to find the default IP values, which specify the destination addresses on a network path. Another way is to use one of the numerous commercial trace route software programs. The trace route tracks a packet from all computers on a delivery path and reports all the router hops along the way. In this way the network topology is discovered.

There are a number of principal ways to compromise routers. Promiscuous mode corruption involves a promiscuous router, which can monitor and redirect traffic to and from other routers. The router will pass all traffic it receives in a random sequence. This happens when an attacker can masquerade as a “super-user” with software control privileges. Many router operating systems make super-user privileges available for maintenance or for software updating reasons.

In router table attacks, an attacker creates messages that look legitimate, and then they can be inserted into the routing table.

During router information attacks, “route poisoning” is used to prevent routing loops within networks. A hop count will indicate to other routers that a route no longer is reachable and should be removed from their respective routing tables. The desired destination for packets will cease to function.

Another tactic is the shortest path attack. Each router passes the status of its links to its neighbors, which in turn forward this information to other routers in the network. As a result of such passing, each router has the link information for all other routers and eventually has the picture of the entire network topology. In a compromised table, the calculated shortest paths will be incorrect, and the shortest path will be purged.

Border gateway attacks exploit the fact that the border gateway protocol does not ensure data integrity and does not provide source authentication. This protocol is the core routing protocol of the Internet, but it can be tampered with.

Border gateway poisoning makes use of router vulnerabilities. Various attacks can be launched to compromise the routing. A special case is the “Black Hole” attack in which the router directs a packet to a network where packets enter but do not come out.

The Internet infrastructure consists of a web of links that connect devices—switches and routers—that have the logical capability to keep redirecting traffic as it travels from origin to destination. The design of the Internet was to engineer this connectivity at the lowest cost possible to central organizations, such as telecommunications carriers, while making tradeoffs that did not favor security. The original engineering of the Internet left it to other remedies, such as virus protection software and firewall equipment, to provide local security assurance.

With the emerging threats of cyberattacks, one can question whether retaining the existing tradeoffs between spending less on the Internet infrastructure and then boosting investments on local protection remains the best way for defending military networks.

Internet communications can be seen as the passage of messages through layers of OSI protocols, as a transaction progresses from entry into an Internet switch until it arrives at its termination on the user’s end. The OSI model defines the entire path of an IP packet. OSI describes the standards that specify the electrical protocols to which all transactions must conform. This approach defines the processing of transactions into seven layers. From top to bottom they are the application, presentation, session, transport, network, datalink and physical layers.

The OSI layered approach makes it possible for each subordinate layer to provide services to the next higher layer as a transaction is converted from lower to higher levels of abstraction. All of these abstractions travel from layer to layer as a series of binary bits because that is the only way microprocessors can handle the passage of a message as it traverses from layer to layer. All of the layers are interdependent; if the datalink or the network layers are compromised, any of the other layers will not be aware of this and communications on the Global Information Grid, or GIG, could cease to function.

Masquerading by the attacker, in many forms, is the root cause for Internet infrastructure attacks. The attacker

either spoofs or disguises information, which then is inserted into switches and routers. When that happens, the network is compromised and can be fixed only through actions that mitigate the intrinsic Internet defects.

The remedy for all the masquerading is the authentication of transactions as well as the vigilance of the operators in the network operating centers to counter attackers' disguises. Though the fundamental protocols of the Internet remain insecure, preventive measures can be taken provided that the thousands of defenders are better organized than the people who are waging the attacks.

Defending the Internet infrastructure is an unequal contest. The attackers benefit from millions of local failures because they can gain knowledge every time they learn about the defenders. The aggressors do not need much money because they use the free Internet, and their software tools can be easily acquired. The tools can be reconfigured to adapt to changing conditions. The defenders meanwhile are tied down by the technologies that must cover the entire network. They are shackled by budgetary limitations that cannot flex for rapid responses because protective measures must cover millions of potential points of exposure. This is why the defenders must rely on superior organization and on human intelligence for rapid responses to unexpected threats after their technological means become insufficient.

The security of the Internet remains the most advanced form of asymmetric arms race. Improved countermeasures by thousands of defenders have to compete against the new schemes devised by a handful of unconventional attackers to corrupt the Internet. This contest takes place not only in the form of technological countermeasures, but also in the form of superior competence of the defenders to maintain operations without error, negligence or acts of omission.

People must accept that the Internet infrastructure is faulty and will remain so for the foreseeable future. It will take an exceptional Cyber Command, staffed by exceptional personnel, to safeguard U.S. military interests against failure that could have devastating consequences.

Paul A. Strassmann is distinguished professor of information science at GeorgeMasonUniversity and the former director of defense information for the Office of the Secretary of Defense.