July 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

BORDER GATEWAY PROTOCOL SECURITY

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The Border Gateway Protocol (BGP) may not be familiar to the average user, but it plays a critical role in the effective operation of the Internet. BGP has been used since the commercialization of the Internet to update routing information between major systems. This routing function makes it possible for systems connected to the Internet to receive and transmit traffic correctly, and to deliver electronic mail and web page transmissions efficiently to users.

Because BGP performs a vital task in keeping the Internet running smoothly, the security of BGP routers is a high-priority concern for organizations. Many organizations do not directly operate BGP routers—the organizations use Internet service providers (ISPs) to handle the routing functions—but other large organizations with extensive networks operate their own routers that run BGP and other routing protocols.

A new guide that provides information on BGP and the methods available to improve the security of BGP routers was recently issued by the Information Technology Laboratory at the National Institute of Standards and Technology (NIST). While primarily directed toward helping federal agencies carry out their responsibilities under the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347), the new guide is also available to private sector organizations that wish to use it.

NIST Special Publication (SP) 800-54, *Border Gateway Protocol Security*

Issued in June 2007, NIST SP 800-54, *Border Gateway Protocol Security: Recommendations of the National Institute of Standards and Technology*, was written by Rick Kuhn, Kotikalapudi Sriram, and Doug Montgomery. The publication explains the structure and the functions of BGP in terms that will enable those who are not familiar with the protocol to understand its use in networking. Potential attacks that threaten the security of BGP functions, the countermeasures that are available to thwart attacks, and their associated costs and benefits are discussed in detail in the guide. The emphasis is on countermeasures that can be applied without significant additions or changes to equipment. NIST SP 800-54 identifies specific recommendations that help decision makers select the measures that can be deployed rapidly and that will significantly improve routing security.

The appendices to NIST SP 800-54 contain an extensive reference list of in-print and online resources, including references to the voluntary industry standards that have been developed primarily by the Internet Engineering Task Force (IETF) to define BGP. Also included in the appendices are an acronym list, definitions of the terms used in the publication, and a table summarizing BGP state transitions.

NIST SP 800-54 is available from NIST's website at http://csrc.nist.gov/publications/nistpubs/index.html.

BGP Security

BGP, a routing protocol, has an important role in enabling the systems that are connected to the Internet to receive and transmit traffic correctly. Each network

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since August 2006:

- *Protecting Sensitive Information Processed and Stored in Information Technology (IT) Systems, August 2006*
- *Forensic Techniques: Helping Organizations Improve Their Responses to Information Security Incidents, September 2006*
- *Log Management: Using Computer and Network Records to Improve Information Security, October 2006*
- *Guide to Securing Computers Using Windows XP Home Edition, November 2006*
- *Maintaining Effective Information Technology (IT) Security Through Test, Training, and Exercise Programs, December 2006*
- *Security Controls for Information Systems: Revised Guidelines Issued by NIST, January 2007*
- *Intrusion Detection and Prevention Systems, February 2007*
- *Improving the Security of Electronic Mail: Updated Guidelines Issued by NIST, March 2007*
- *Securing Wireless Networks, April 2007*
- *Securing Radio Frequency Identification (RFID) Systems, May 2007*
- *Forensic Techniques for Cell Phones, June 2007*

communication, such as sending and receiving mail and viewing websites, is accomplished through messages called packets. These packets contain the source and destination addresses for the transactions, but the packets do not go directly from a user's computer to their destination. Many intermediate systems may be involved in the transmission of the packets, and not all of the packets follow the same path from source to destination. The packets pass through systems and are forwarded to other systems, based on the destination address and information contained in a routing table. For example, the routing table could state that packets with a destination of A can be sent to system H, which will then forward the packets to their destination, possibly through other intermediate nodes.

The routers, computers, and other components within a single administrative domain compose an autonomous system (AS). A university, a company network, and an ISP are examples of a single AS. In some cases, corporate networks tied to the ISP may also be part of the ISP's AS, although some aspects of the network administration are not under the control of the ISP.

AS numbers are managed by the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization established by the U.S. Department of Commerce, which authorizes Internet registration organizations to assign AS numbers. As of May 2007, the Internet included more than 25,000 registered autonomous systems.

Because the systems connected to the Internet change frequently, the most efficient paths between systems and the routing tables must be updated on a regular basis. The information in the routing tables has also increased considerably with the growth of the Internet.

Each AS has many routers for internal communication and one or more routers for communications outside the local network. Internal routers use interior BGP (IBGP) to communicate with each other, and external routers use external BGP (EBGP). Two routers that have established a connection for exchanging BGP information are referred to as *peers*. BGP peers use the Transmission Control Protocol (TCP), the same protocol used for e-mail and web page transmissions, to exchange routing information in the form of address prefixes that the routers recognize, as well as additional data that is used to select the best route for the information.

Who We Are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

Risks and Attacks

If BGP fails to carry out the routing function, portions of the Internet may become unusable for periods of time ranging from minutes to hours. Most of the risk to BGP comes from accidental failures, but there is also a significant risk that attackers could disable parts or all of networks, disrupting communications, commerce, and possibly putting lives and property in danger.

BGP, which was developed before security became a serious issue for the Internet, does not have a built-in authentication mechanism to ensure that a message is really from the AS that is shown as the source in messages. As a result, BGP may be vulnerable to attacks, despite extensions that have been developed to improve its security. Many of the methods developed over the years to improve the dependability of BGP also contribute to security against outside attackers.
Attacks on BGP could cause a loss of connectivity between critical portions of the Internet; that is, e-mail, e-commerce, and web accesses would not function. Because of the volume of commercial transactions conducted over the Internet, plus increasing use of the Internet for voice communications (voice over IP [VOIP]), such an outage could have a significant impact on the economy and possibly interrupt critical functions such as emergency services communications. The outage could be either widespread, affecting large portions of the Internet, or a targeted denial of service attack against a particular organization's network.
Another security concern is the potential loss of confidentiality of information if packets are misrouted. Internet communication is not secure unless special measures are taken, such as encryption, and most users do not encrypt e-mail or other traffic. An eavesdropper could mount an attack by changing routing tables to redirect traffic through nodes that can be monitored. The attacker could thus monitor the contents or source and destination of the redirected traffic or modify it maliciously.
Insider attacks, either malicious or accidental, are another concern. Threats from insiders require extra measures of access control enforced within an organization.

Countermeasures

When developed originally, BGP had no built-in security functionality. However, the security of BGP can be improved through the application of countermeasures, which are described in NIST SP 800-54. NIST provides approximate ratings of countermeasures for effectiveness and cost as Low (L), Medium (M), or High (H). These ratings are subjective and intended as an approximate guide only. Actual cost and effectiveness will vary with the installation. Comprehensive BGP security solutions have not yet emerged, and current "best common practices" are somewhat overlapping, confusing in scope and applicability, and often neglect cost/benefit trade-offs.

Recovery and Restart

Improving the dependability of some systems subject to denial of service attacks can be done by increasing the difficulty of an attack or reducing the time needed to recover from such an attack. In terms of system availability, the first option corresponds to increasing system uptime, *U*, while attack recovery corresponds to reducing downtime, *D* (ignoring other sources of downtime). Availability is

calculated as $U/(U + D)$. For example, a system with uptime of 1000 hours (over a measurement period) and a downtime of 1 hour has availability of 1000/1001 = 99.9%. If recovery time can be reduced to 0.1 hours, availability improves significantly, to 99.99%. By contrast, if recovery time remains at 1 hour, defenses would have to be strengthened to hold off attacks for 10,000 hours to achieve the same 99.99% availability. Reducing the time needed to recover from a denial of service attack can improve BGP availability and, for some attacks, may be a more cost-effective strategy than hardening defenses. Quicker recovery also means less disruption to other parts of the network.

NIST Recommendations for the Security of BGP Routers

NIST recommends that organizations adopt a program of best practices to help protect BGP routers. The recommendations, which are detailed in NIST SP 800-54, can be implemented on current BGP routers to improve security.

Following is a summary of NIST's technical recommendations; in some cases, references are provided to specific sections of the BGP guide, which explains in more detail the rationale for the actions and the recommended steps to be taken. These steps alone are not a complete defense against all threats, and security administrators and decision makers should select and apply these methods based on their unique needs.

- Establish and use access control lists. This feature is available on nearly all routers (see Section 4.2 of the publication).

- Use BGP graceful restart, when available with latest manufacturer-recommended default settings (see Section 5.1).

- Use BGP peer authentication. Authentication is one of the strongest mechanisms for preventing malicious activity. Use Internet Protocol Security (IPsec) or BGP MD5 authentication mechanisms, if available (see Section 4.5 and Section 4.6).
- Use prefix limits to avoid filling router tables. Routers should be configured to disable or terminate a BGP peering session and issue warning messages to administrators when a neighbor sends in excess of a preset number of prefixes (see Section 4.2).

- Only allow peers to connect to port 179. The standard port for receiving BGP session OPENs is port 179, so attempts by peers to reach other ports are likely to indicate faulty configuration or potential malicious activity.

- Configure BGP to allow announcing only designated netblocks. This option will prevent the router from inadvertently providing transit to networks not listed by the autonomous system (AS) (see Section 2.3).

- Filter all bogon (an address that is reserved but not yet registered) prefixes. These prefixes (see Section 4.2.2) are invalid, so they should not appear in routes. Filtering them reduces load and helps reduce the ability of attackers to use forged addresses in denial of service or other attacks.

- Where feasible, routers should do ingress filtering (filtering of incoming prefixes) on peers (see Section 4.2, including 4.2.5).

- Do not allow over-specific prefixes. Requiring routers to maintain large numbers of very specific prefixes can place excessive load on system resources. Recommendations vary as to what prefixes should be considered "over-specific," but a reasonable criterion could be those with prefix addresses in the range of /24 to /30. (IP address blocks are given in the Classless Interdomain Routing [CIDR] format, *A/n*, where *A* is an IP address and *n* is the prefix length.)
- Turn off fast external failover to avoid major route changes due to transient failures of peers to send keepalives. The "fast external failover" feature was designed to allow rapid failover to an alternate system when a link goes down. Without this feature, failover would not occur until BGP keepalive timers would permit recognition that the line had failed. It is not uncommon for lines to drop BGP sessions and then return. This is referred to as route flapping (see Section 3.2.4). Frequent flapping can trigger flap damping in upstream peers. Due to fast external failovers, flap damping would occur at upstream routers, which in turn results in prolonged peer-prefix unreachability and system instability. So turning off fast external failover normally represents a positive trade-off in today's Internet.

- Trade-offs are involved with route flap damping (RFD), and current research suggests that it contributes to a number of problems. It should not be enabled unless the organization has a strong case for its use. See Section 3.2.4 for a discussion of RFD. If route flap damping is used, longer prefixes should be damped more aggressively. Longer prefixes tend to be less stable, so longer RFD times are preferable. Sample half-time periods of RFD decay are as follows:

- less than /21 - manufacturer recommendation (conventional default is 15 minutes);
- /21 and shorter prefixes - not more than 30 minutes;
- /22 to /23 prefixes - not more than 45 minutes; and
- /24 and greater prefixes - not more than 60 minutes.

- Do not use route flap damping for netblocks that contain domain name system (DNS) root servers.

These networks are normally the most stable and can be expected to remain operating in all but the most exceptional circumstances. Damping these netblocks would therefore be likely to have more negative results than benefits. DNS root servers are also critical for Internet operations, so degraded access to them could cause widespread disruption of network operations.

- Use soft reconfiguration, where practical. Normally a change in policy requires BGP sessions to be cleared before the new policy can be initiated, resulting in a need to rebuild sessions with consequent impact on routing performance. Thus, spoofed policy changes could be used for a denial of service attack, even if the policy changes themselves do not violate AS rules. Soft reconfiguration allows new policies to be initiated without resetting sessions. It is done on a per-peer basis and can be set up for either inbound or outbound or both (for updates from and to neighbors, respectively).

- Record peer changes. Log whenever a peer enters or leaves Established state, providing useful records for debugging or audit trails for investigating possible security problems.

Future Activities

A variety of proposals have been introduced in standards bodies for more comprehensive approaches to BGP security, but issues are not yet settled as to which, if any, of these proposals will be adopted by the producers and consumers of routing equipment. When the extensions become more widely accepted, NIST will consider developing updated recommendations for BGP security.

More Information

NIST publications assist organizations in planning and implementing a comprehensive approach to information security, including basic planning functions, the risk management process, and the selection, implementation, and assessment of security controls.

Publications dealing specifically with network protocol issues include:

NIST SP 800-77, *Guide to IPsec VPNs*, by Sheila Frankel, Karen Kent, Ryan Lewkowski, Angela D. Orebaugh, Ronald W. Ritchey, and Steven R. Shama, explains security controls that can be implemented to protect Transmission Control Protocol/Internet Protocol (TCP/IP) network communications.

NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, by C. Michael Chernick, Charles Edington III, Matthew J. Fanto, and Rob Rosenthal, discusses computer communications architectural concepts and the foundations of communications security.

These publications and other security-related publications, including Federal Information Processing Standards (FIPS), are available from NIST's website http://csrc.nist.gov/publications/nistpubs/index.html.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.