CHAPTER 1

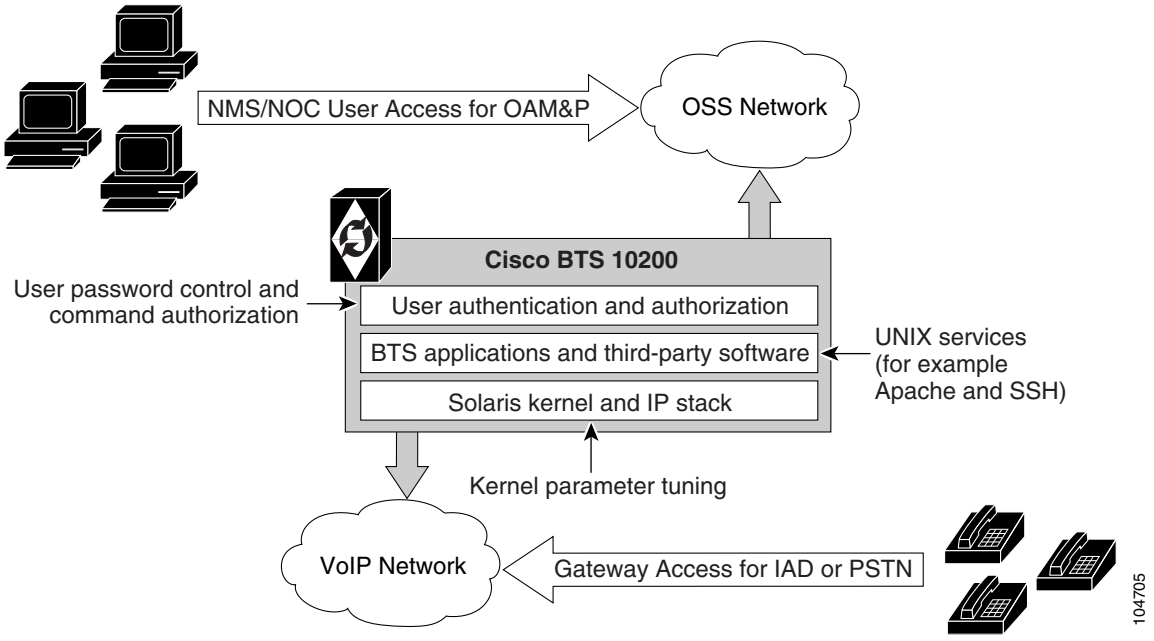
Behaviors and Attributes

June 21, 2007 OL-12437-01

This chapter details the behaviors and attributes of the various security packages in the Cisco BTS 10200 Softswitch. The sources for the items are derived from many dynamic sources. Included in these sources are security bulletins from third-party vendors to the Cisco BTS 10200 Softswitch as well as security agencies and open source organizations.

Security is an important part of the Cisco BTS 10200 Softswitch. The Cisco BTS 10200 Softswitch has interfaces to customer premise equipment (CPE) as well as northbound Operations Support System (OSS) interfaces. All of these interfaces are subject to attacks. In addition, users who are allowed onto the Cisco BTS 10200 Softswitch can also find ways to exploit applications that can lead to service-affecting situations. Therefore, many precautions are taken to ensure the solidity of the Cisco BTS 10200 Softswitch defenses while avoiding a system that is difficult to manage.

Figure 1-1 Cisco BTS 10200 Softswitch Access and Related Security



Adapter and User Security

This section describes requirements that generally involve adapter and user level of security. In the Cisco BTS 10200 Softswitch, adapters are any external, northbound interfaces of the Cisco BTS 10200 Softswitch. However, some extrapolated requirements involve adapter technology based on the current deployment:

- Support termination of a session once a provisionable inactivity timeout has occurred. An event report is issued upon each timeout expiry. The inactivity time ranges from 10 to 30 minutes.
- Restrict access as “root” to the Cisco BTS 10200 Softswitch in all cases except Cisco TAC and customer “administrator”. This is a broad statement that includes the addition of command-line interface (CLI) commands to help manage the system. In addition, UNIX services are restricted to harden the operating system (OS). The service restriction is listed in the Solaris OS Security and BTShard Package section. The process of restricting root access is an ongoing process.
- Use of “sudo" is acceptable and the formal Sun-built and packaged version is located in /opt/sfw/bin/.

Solaris OS Security and BTShard Package

This section details the security packages for the Cisco BTS 10200 Softswitch OS. These packages are automatically installed at installation. These packages are derived from both Sun Microsystems security bulletins and Cisco internal policies for safety of the OS and its applications. All services can be reactivated for the lifetime of the current kernel instance. All settings are reset on reboot of the kernel. These settings are contained in the BTShard Solaris package delivered with the Cisco BTS 10200 Softswitch.

- Remove unnecessary UNIX systems services. These services are listed below. Management of these facilities must allow for each service to be enabled or disabled on an individual basis. This service management must also be accomplished through the Cisco BTS 10200 Softswitch adapter interface.
  - FTP—FTP server is disabled and SFTP (Secure FTP) should be used. This impacts the Bulk Data Provisioning interface. It does not impact the Billing Bulk Data transfer. The FTP client code will still be available on the EMS node.
  - Telnet—This terminal protocol is disabled and SSH (Secure Shell) should be used. The telnet server and client code are still available on the EMS node.
  - Echo—This service is to be disabled. This capability has been replaced with Internet Control Message Protocol (ICMP) “ping” facilities.
  - Discard—This service is to be disabled.
  - Printer—This service is to be disabled. No printer services are supplied in the Cisco BTS 10200 product description.
  - Daytime—This service is to be disabled.
  - Chargen—This service is to be disabled.
  - SMTP—This service is to be disabled.
  - Time—This service is to be disabled.
  - Finger—This service is to be disabled. No network user facilities are required. The Cisco BTS 10200 tracks users internally and on a single BTS basis.

  - Sun RPC—This service is to be disabled. This may be enabled in a lab environment for Tooltalk usage in debugging application programs.
  - Exec—This service is to be disabled.
  - Login—This service is to be disabled.
  - Shell—This service is to be disabled. This may be required for some lab activity; however, there is no field usage for rlogin, rcp, and rsh facilities.
  - UUCP—This service is to be disabled.
  - NFS—This service is to be disabled.
  - Lockd—This service is to be disabled.
  - X11—This service is available for the near term *only*.
  - DTSCP—This service is to be disabled.
  - Font-services—This service is to be disabled.
  - HTTP—This service is to be enabled. This is used by the Cisco BTS 10200 Softswitch to offer results of report generation. This will migrate to HTTPS.
- The following UNIX accounts are to be LOCKED but not removed from the system: lp, uucp, nuucp, nobody, listen, and any other Cisco support accounts not used in the normal course of field operation. Services managed by root are the only accounts allowed to utilize one of these identities. This is the default behavior.
- Modifications to the Solaris kernel parameters were made to close potential breeches in the OS. These types of security precautions are most often geared toward "denial of service" attacks. These types of attacks create situations that degrade the performance of a system and as a result, prohibit the critical applications from delivering the service they are designed to provide.
- The TCP protocol uses random initial sequence numbers.
- All failed login attempts are logged.
- The following users are not allowed direct FTP access to the machine: root, daemon, bin, sys, adm, nobody, and noaccess.
- A root user cannot Telnet directly to the machine. Direct root user access is granted to the console only. A user who wants to access the root account must use the **su** command from a nonprivileged account.
- The break key (<STOP> <A>) on the keyboard is disabled.
- IP_FORWARD_DIRECTED_BROADCASTS—This option determines whether to forward broadcast packets directed to a specific net or subnet, if that net or subnet is directly connected to the machine. If the system is acting as a router, this option can be exploited to generate a great deal of broadcast network traffic. Turning this option off helps prevent broadcast traffic attacks. The Solaris default value is 1 (True). For example:

  ```
  ip_forward_directed_broadcasts=0
  ```

- IP_FORWARD_SRC_ROUTED—This option determines whether to forward packets that are source routed. These packets define the path the packet should take instead of allowing network routers to define the path. The Solaris default value is 1 (True). For example:

  ```
  ip_forward_src_routed=0
  ```

- IP_IGNORE_REDIRECT—This option determines whether to ignore the ICMP packets that define new routes. If the system is acting as a router, an attacker may send redirect messages to alter routing tables as part of sophisticated attack (man-in-the-middle attack) or a simple denial of service. The Solaris default value is 0 (False). For example:

  ```
  ip_ignore_redirect=1
  ```

- IP_IRE_FLUSH_INTERVAL—This option determines the period of time at which a specific route will be kept, even if currently in use. Address Resolution Protocol (ARP) attacks may be effective with the default interval. Shortening the time interval may reduce the effectiveness of attacks. The default interval is 1200000 milliseconds (20 minutes). For example:

  ```
  ip_ire_flush_interval=60000
  ```

- IP_RESPOND_TO_ADDRESS_MASK_BROADCAST—This option determines whether to respond to ICMP netmask requests which are typically sent by diskless clients when booting. An attacker may use the netmask information for determining network topology or the broadcast address for the subnet. The default value is 0 (False). For example:

  ```
  ip_respond_to_address_mask_broadcast=0
  ```

- IP_RESPOND_TO_ECHO_BROADCAST—This option determines whether to respond to ICMP broadcast echo requests (ping). An attacker may try to create a denial of service attack on subnets by sending many broadcast echo requests to which all systems will respond. This also provides information on systems that are available on the network. The Solaris default value is 1 (True). For example:

  ```
  ip_respond_to_echo_broadcast=1
  ```

- IP_RESPOND_TO_TIMESTAMP—This option determines whether to respond to ICMP timestamp requests which some systems use to discover the time on a remote system. An attacker may use the time information to schedule an attack at a period of time when the system may run a cron job (or other time-based event) or otherwise be busy. It may also be possible predict ID or sequence numbers that are based on the time of day for spoofing services. The Solaris default value is 1 (True). For example:

  ```
  ip_respond_to_timestamp=0
  ```

- IP_RESPOND_TO_TIMESTAMP_BROADCAST—This option determines whether to respond to ICMP broadcast timestamp requests which are used to discover the time on all systems in the broadcast range. This option is dangerous for the same reasons as responding to a single timestamp request. Additionally, an attacker may try to create a denial of service attack by generating many broadcast timestamp requests. The default value is 1 (True). For example:

  ```
  ip_respond_to_timestamp_broadcast=0
  ```

- IP_SEND_REDIRECTS—This option determines whether to send ICMP redirect messages which can introduce changes into the routing table of the remote system. It should only be used on systems that act as routers. The Solaris default value is 1 (True). For example:

  ```
  ip_send_redirects=0
  ```

- IP_STRICT_DST_MULTIHOMING—This option determines whether to enable strict destination multihoming. If this is set to 1 and ip_forwarding is set to 0, then a packet sent to an interface from which it did not arrive will be dropped. This setting prevents an attacker from passing packets across a machine with multiple interfaces that is not acting a router. The default value is 0 (False). For example:

  ```
  ip_strict_dst_multihoming=1
  ```

- TCP_CONN_REQ_MAX_Q0—This option determines the size of the queue containing half-open connections. This setting provides protection from SYN flood attacks. Solaris 2.6 and 7 (and 2.5.1 with patch 103582-12 and higher) include protection from these attacks. The queue size default is adequate for most systems but should be increased for busy web servers. The default value is 1024. For example:

  ```
  tcp_conn_req_max_q0=4096
  ```

- The following startup files are removed from the level "3" runtime environment of the Cisco BTS 10200 Softswitch. These services can still be started manually if required in laboratory circumstances. They are not required for field operations.
  - S71rpc
  - S73cachefs.daemon
  - S73nfs.client
  - S74autofs
  - S80lp
  - S80spc
  - S88sendmail
  - S93cacheos.finish
  - S99dtlogin

CERT Advisories and Network Security

This section covers the network security requirements for the Cisco BTS 10200 Softswitch. These requirements are derived from CERT and Cisco Systems internal policy. These requirements cover any access to the Cisco BTS 10200 Softswitch by IP interfaces, as well as all console access. These items are addressed in the BTSossh Solaris package and the SMCapache Solaris package that are delivered with the Cisco BTS 10200 Softswitch.

- Open Secure Shell (OpenSSH) must be updated to include the following CERT advisories. These are resolved in the current OpenSSH version 3.4.p1.
  - CA-2002-24—The description of the problem from the CERT-2002-24 advisory is: "The CERT/CC has received confirmation that some copies of the source code for the OpenSSH package were modified by an intruder and contain a Trojan horse." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2002-24.html.
  - CA-2002-18—The description of the problem from the CERT-2002-18 advisory is: "There are two related vulnerabilities in the challenge response handling code in OpenSSH versions 2.3.1p1 through 3.3. They may allow a remote intruder to execute arbitrary code as the user running sshd (often root)." The first vulnerability affects OpenSSH versions 2.9.9 through 3.3 that have the challenge response option enabled, and use SKEY or BSD_AUTH authentication. The second vulnerability affects PAM modules using interactive keyboard authentication in OpenSSH versions 2.3.1p1 through 3.3, regardless of the challenge response option setting. For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2002-18.html.
- Open Secure Socket Layer (OpenSSL) must be updated to include the following CERT advisory. This is corrected in version 0.9.8 or later. This is contained in the BTSossl Solaris package bundled with BTSossh in the Cisco BTS 10200 Softswitch.

  - CA-2002-23—The description of the problem from the CERT-2002-23 advisory is: "There are four remotely exploitable buffer overflows in OpenSSL. There are also encoding problems in the ASN.1 library used by OpenSSL. Several of these vulnerabilities can be used by a remote attacker to execute arbitrary code on the target system. All can be used to create denial of service." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2002-23.html.
  - CERT-2003-24—The description of the problem from the CERT-2003-24 advisory is: "There is a remotely exploitable vulnerability in a general buffer management function in versions of OpenSSH prior to 3.7.1. This may allow a remote attacker to corrupt heap memory which could cause a denial-of-service condition. It may also be possible for an attacker to execute arbitrary code." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2003-24.html.
  - CERT-2003-26—The description of the problem from the CERT-2003-26 advisory is: "There are multiple vulnerabilities in different implementations of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These vulnerabilities occur primarily in Abstract Syntax Notation One (ASN.1) parsing code. The most serious vulnerabilities may allow a remote attacker to execute arbitrary code. The common impact is denial of service." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2003-26.html.

- The Apache web server must be updated to include the following CERT advisory. This is corrected in version 2.0.39 or later. The Solaris command **pkginfo -l SMCapache** indicates the current release level of the Apache package in the Cisco BTS 10200 Softswitch.
  - CA-2002-17—The description of the problem from the CERT-2003-26 advisory is: "There is a remotely exploitable vulnerability in the way that Apache web servers (or other web servers based on their source code) handle data encoded in chunks. This vulnerability is present by default in configurations of Apache web server versions 1.2.2 and later, 1.3 through 1.3.24, and versions 2.0 through 2.0.36. The impact of this vulnerability is dependent upon the software version and the hardware platform the server is running on." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2002-17.html.

Secure FTP (SFTP) is the default method for bulk transfer of provisioning data to the Cisco BTS 10200 Softswitch. FTP is disabled as a default. The SFTP service is provided in the BTSossh Solaris package included in the Cisco BTS 10200 Softswitch.