Avaya Solution & Interoperability Test Lab

Application Notes for the InfoPlus Security Audit with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for InfoPlus Security Audit, by Bristol Capital Inc., to successfully interoperate with Avaya Communication Manager.

InfoPlus Security Audit is a remote solution that interrogates an Avaya Communication Manager system. It collects software data on how the PBX system is being used or misused, and flags system security concerns. The resulting InfoPlus Security Audit report is not only a detailed summary of how the PBX system is programmed, but specifies corrective action to enhance system security. InfoPlus Security Audit is a meaningful reporting tool for security management usage.

Serviceability and performance tests were conducted to assess the reliability of the solution.

Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1 Introduction

InfoPlus Security Audit by Bristol Capital Inc. is a detailed security analysis report of an Avaya Communication Manager system. InfoPlus Security Audit addresses the concerns of possible security weaknesses on the PBX platform, and further specifies how to take corrective action to prevent the security problems. The detailed security output result of Avaya Communication Manager audit is a meaningful reporting tool for security management.

The InfoPlus Security Audit solution is processed by an InfoPlus Central Database system. The InfoPlus Central Database connects to the Avaya Communication Manager platform using a dialup modem connection. The InfoPlus Central Database is challenged during the login process, presents the Server Availability Management Processor (SAMP) interface with the correct login criteria, and gains access to the Avaya Communication Manager SAT command interface. The InfoPlus Central Database then executes a subset of SAT commands specifically targeted for gathering information about the configuration on the Avaya Communication Manager system (see Appendix A for the complete list of SAT commands).

The InfoPlus Central Database manipulates the captured data into a clear and concise format that is presented to Bristol Capital's customer. From the information obtained by the InfoPlus Security Audit solution, Avaya Communication Manager configuration details are clearly organized and visualized. PBX business decisions can be made based on the results of the InfoPlus Security Audit solution.

See Appendix B for the InfoPlus Security Audit Report.

The illustration below describes the network configuration used to compliance test the InfoPlus Security Audit solution. The InfoPlus Central Database gains access to the Avaya Communication Manager platform via a modem interface, thus allowing the InfoPlus Security Audit command-line suite of functions to be executed.

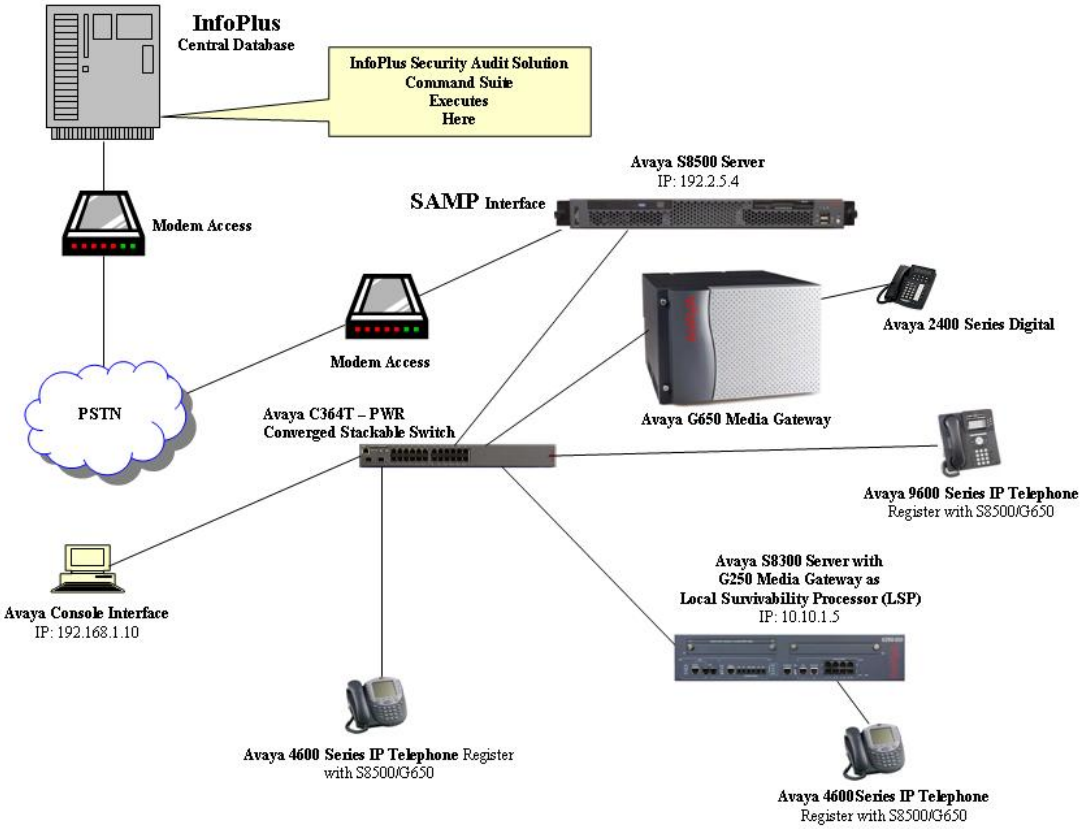


Figure 1 – InfoPlus Test Configuration

2 Equipment and Software Validated

The following table lists the equipment and software versions that were used for compliance testing.

Equipment	Software
Avaya S8500 Server with G650 Media Gateway	4.0.0(R014x.00.0.730.5)
Avaya S8300 Server with G250 Media Gateway	4.0.0(R014x.00.0.730.5)
Avaya 9600 Series IP Telephones	1.20 (H.323)
Avaya 4600 Series IP Telephones	4602: 1.8 (H.323) 4620: 2.8 (H.323)
Avaya 2400 Digital Telephones	
Avaya C363T-PWR Converged Stackable Switch	4.5.14
MultiTech System, Multi*Modem*	
InfoPlus Security Audit Solution	Not Available [1]

[1] InfoPlus software version is for InfoPlus internal use only.

Table 1 – Hardware and Software Components

3 Avaya Communication Manager Configuration

Administration for proper modem connectivity must be performed.

3.1 Avaya Server Availability Management Processor

The Avaya Communication Manager platforms used for the compliance test were an Avaya S8500 Server with G650 Media Gateway and an Avaya S8300 with G250 Media Gateway as a Local Survivability Processor (LSP). The SAMP interface card installed on the S8500 in slot 1, allows for a modem interface connection. When the appropriate hardware and modem are installed, follow the steps below to ensure proper modem setup.

- Telnet to the S8500 system and log into the Linux interface. At the Linux system prompt, enter **sampdial –v**. A response indicating the SAMP interface is functioning should be displayed as below (SAMP OK):

  craft@S8500C> sampdiag -v
  The SAMP is using the Avaya IP address.
  SAMP HWaddress: 00:0F:29:01:4E:28
  SAMP IPaddress: 192.11.13.2 [2]
  HOST IPaddress: 192.11.13.1
  SSH port: 10022
  SSH OK
  HPI OK
  SAMP OK
  craft@S8500C>

- Setup login access for the modem interface by creating a user and assigning the user a password. At the system prompt, enter **rmbuseradd rasaccess** (rasaccess is used in this case)**.**

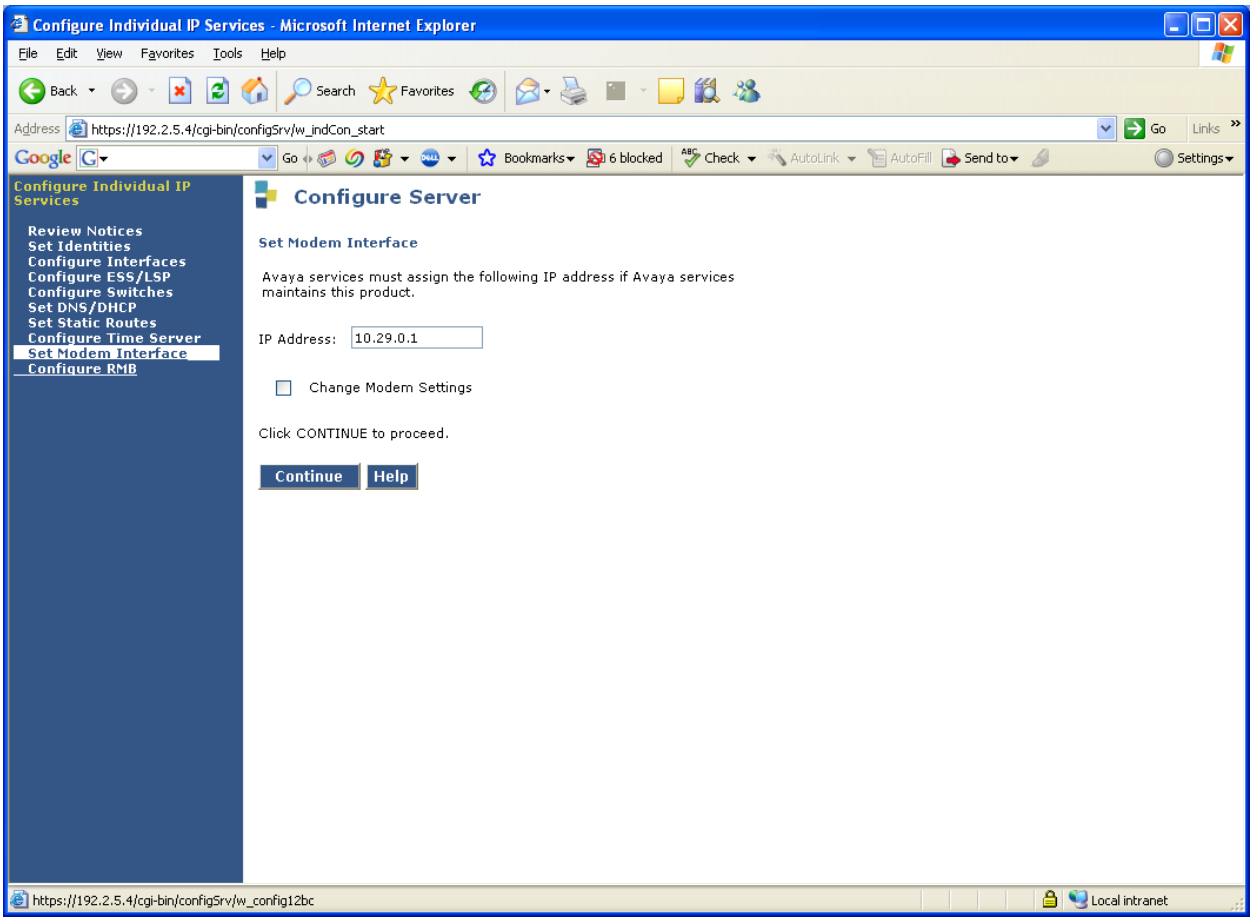
  craft@S8500C>
  craft@S8500C> rmbuseradd rasaccess
  craft@S8500C>

- Again, at the system prompt, enter **rmbpasswd rasaccess.** This will create the first password level challenge encountered by the InfoPlus Central Database processor. The password is not visible when entered.

  craft@S8500C>
  craft@S8500C> rmbpasswd rasaccess
  Enter new password:
  Re-enter new password:
  craft@S8500C>

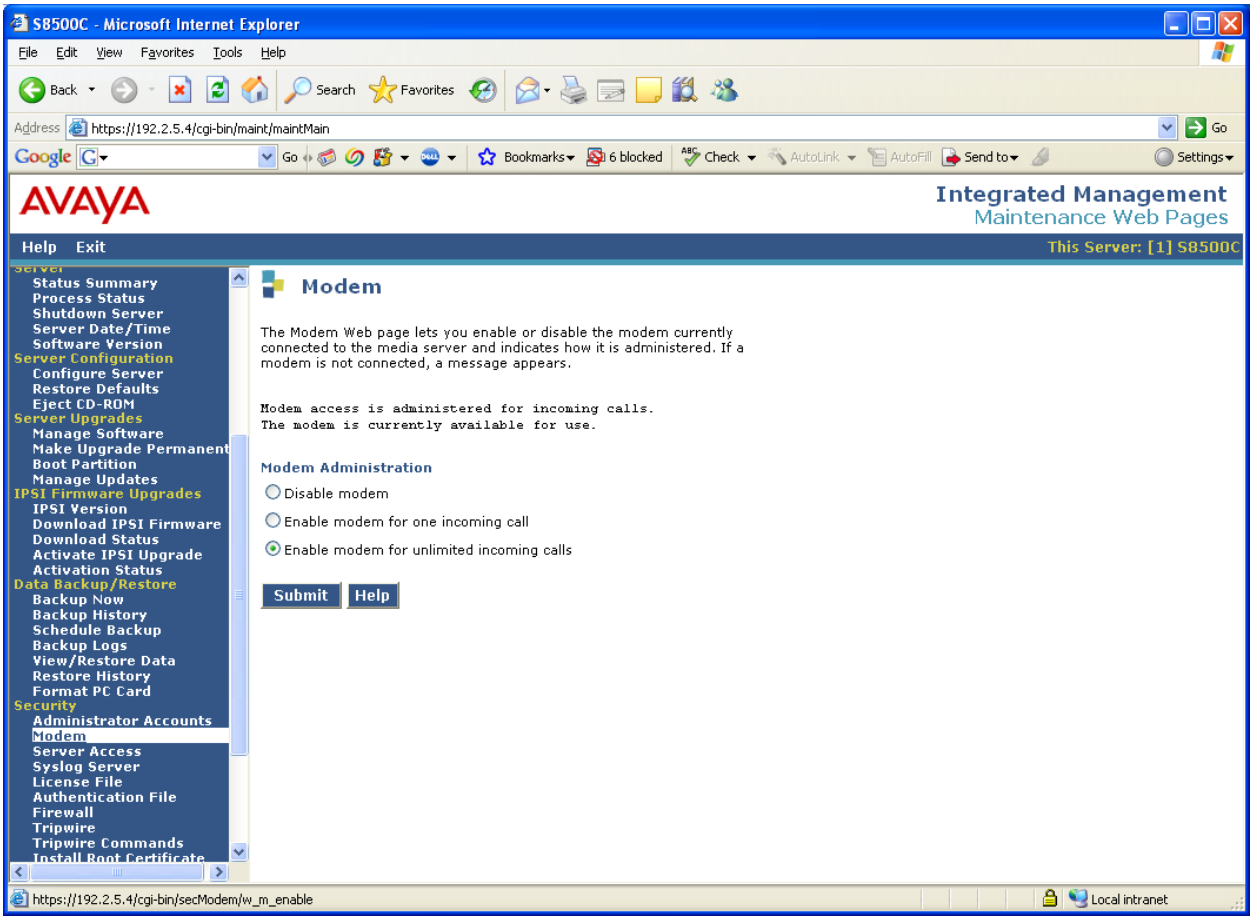
[2] Default IP addresses are listed with the "sampdiag –v" command results.

- Administration of several modem related features must be configured using the Maintenance WEB interface. Launch the Maintenance WEB interface and click on **Configure Server** from the left navigation panel. Continue and under **Configure Individual IP Services,** select **Set Modem Interface** as below. An IP address is assigned for the modem PPP connectivity session. Click and ensure the system updated successfully.



- On the left navigation panel, click on **Modem**. Ensure that **Enable modem for unlimited incoming calls** is enabled. Click **Submit** and ensure that the following message, as displayed below, is obtained:

  Modem access is administered for incoming calls.
  The modem is currently available for use.



4 InfoPlus Security Audit Configuration

The InfoPlus Security Audit solution is not a software package that is configured or operates at the customer premise; therefore the customer does not require any setup knowledge of the InfoPlus Security Audit solution. All the system expertise is completely centralized to the InfoPlus Central Database location.

A pre-determined set of passwords and a network IP address must be known by the InfoPlus system administrator to allow modem access to occur. The Avaya system administrator needs to communicate the following information to InfoPlus:

- Telephone number for modem access
- Remote access modem login
- Remote access modem password
- Assign IP address for "telnet" session
- SAT login access
- SAT login password

5 Interoperability Compliance Testing

Interoperability compliance testing included InfoPlus Central Database connectivity, command-line implementation, and serviceability.

Connectivity between systems was pre-arranged by Avaya and Bristol Capital, whereby logins, passwords, and a modem IP address were setup in the InfoPlus Central Database processor. The InfoPlus Central Database processor dialed into the SAMP interface using the modem login and password, after which a PPP session was created. A telnet to the modem IP address allowed access to the Linux interface. After logging in using the **craft** login and password, the SAT interface was acquired. The InfoPlus Central Database processor runs a command-line suite of functions from this interface.

The serviceability tests introduced modem connectivity failure scenarios. The failures were performed by pulling out the modem telephone line while the InfoPlus Central Database processor was actually in session. Recovery was accomplished by plugging the telephone line back in and restarting the InfoPlus Central Database processor login session. The last command-line entered at the time of the failure was the point of pickup as the set of command-line functions continued.

5.1 Test Results

All command-line functions geared for the InfoPlus Security Audit service passed compliance testing. The output captured and formulated in a value-added concise format, passed compliance testing. Serviceability compliance tests passed.

6 Verification Steps

Compare the output produced by the InfoPlus Security Audit solution with the configuration of the Avaya Communication Manager system.

7 Support

Technical support for Bristol Capital's InfoPlus Security Audit can be obtained by contacting Bristol Capital Inc. at 201-476-0600 or by sending e-mail to support@infoplusonline.com.

8 Conclusion

This Application Note describes what is required to allow Bristol Capital's InfoPlus Security Audit solution to interoperate with Avaya Communication Manager. The result of the interoperability testing is presented in Appendix B.

9 References

This section references the Avaya and Bristol Capital documentation that are relevant to these Application Notes. The Avaya product documentation can be found at http://support.avaya.com, and information regarding InfoPlus Security Audit can be obtained at http://www.infoplusonline.com.

[1] Using the Avaya Server Availability Management Processor (SAMP) - Issue 4), February 2007

10 Appendix A

The categories of the SAT commands run by the InfoPlus Central Database are listed in the following table.

SAT Command Categories by InfoPlus Service
• Extensions • Config All • Stations • Data Modules • Attendants • Announcements • Trunk Groups • Trunk Group Details • Config DS1 • Status System All Cabinets • Cabinets • Capacities • Config Software • Offer • Customer Options • Aliases • Media Gateways • Media Gateway Details

A full set of actual SAT commands for the InfoPlus suite is listed in the following table.

Command Category	Command Syntax
Extension List:	list extension-type
Abbreviated Dialing Groups:	list abbrev group
Abbreviated Dialing Groups Details:	disp abbrev system disp abbrev group X Where X is each group listed by “list abbrev group”
Abbreviated Dialing Personal:	list abbrev personal

Command Category	Command Syntax
Abbreviated Dialing Personal Details:	disp abbrev personal X list Y Where X and Y are all the possible values from "list abbrev personal"
Announcements Detail:	disp announcements
Attendants Detail:	display attendant X Where X is 1 through 28 inclusive
COS Detail:	disp COS
COR Detail:	display COR X Where X can be 0 through 996 inclusive. (For Security Audits, retrieve every COR that exists. For all other services, intelligently determine those that are in use by analyzing Authorization Codes, Extensions, Remote Access and Trunks)
ARS Analysis:	list ars analysis
AAR Analysis:	list aar analysis
Config All:	list config all
Config DS1:	list config ds1
Config Software:	list config software
Coverage Answer:	list coverage answer
Coverage Answer Details:	disp coverage answer X Where X is each value from "list coverage answer"
Coverage Path:	list coverage path
Coverage Path Detail:	disp coverage path X Where X is each value from "list coverage path"
Remote Coverage Path Details:	disp cov rem OR (if switch needs an Identifier) disp cov rem X Where X is each value from 1-10 inclusive
Data Modules:	list data
Hunt Groups:	list hunt-group
Hunt Group Details:	disp hunt-group X Where X is each value from "list hunt-group"
Intercom Groups:	list intercom-group

Command Category	Command Syntax
Intercom Group Details:	disp intercom-group X Where X is each value from "list intercom-group"
Pickup Groups:	list pickup-group
Pickup Group Details:	disp pickup-group X Where X is each value from "list pickup-group"
Route Patterns:	list route-pattern
Route Pattern Detail:	display route-pattern X Where X is each value from "list route-pattern"
Trunk Groups:	list trunk-group
Trunk Group Details:	disp trunk-group X Where X is each value from "list trunk-group"
Paging:	disp paging loudspeaker
Capacities:	disp capacities
Offer:	display system-parameters offer
Partitioned Group:	list partitioned-group
Partition Route Table:	list partition-route-table
Toll:	list toll all
Bridged:	list bridge X Where X = each extension found in the Extension list
Stations:	list station
Logins:	list login
Login Details:	display login X Where X is each value from "list login"
Permissions:	display permission Where X is each value from "list login"
Features:	display system-parameters feature
Maintenance:	display system-parameters maintenance
Security:	display system-parameters security
Dial Plan:	display dialplan analysis
IP Services:	display ip-services
CDR:	display system-parameters cdr
Feature Access Codes:	display feature-access-codes

Command Category	Command Syntax
Aliases:	display alias station
Remote Access:	display remote-access
Time of Day Routing:	display time-of-day X Where X is every value from 1-8 inclusive
Report Schedule:	list report-scheduler
Authorization Codes:	list authorization-code
Agent LoginIDs:	list agent-loginID
Vectors:	list vector
Vector Details:	display vector X Where X is each value from "list vector"
Media Gateways:	list media-gateway
Media Gateway Details:	display media-gateway X Where X is each value from "list media-gateway"
Listed Directory:	disp listed-directory-number
Alternate FRL:	disp alternate-frl
Traffic Measurement:	disp meas-selection trunk-group disp meas-selection route-pattern
Tenants:	display tenant X (Only if Tenant Partitioning is enabled in Customer Options) Where X is each value from 1-100 inclusive
Off PBX Feature Name Extensions:	display off-pbx-telephone feature-name-extensions
Status System Cabinets:	status system all-cab
Cabinet Details:	status cabinet X Where X is each value from "list config-all"
Call Forwarding:	list call-forwarding
ASG History:	list asg-history
VDNs:	list vdn
VDN Details:	display vdn X Where X is each value from "list vdn"
Off PBX Station Mapping:	list off-pbx-telephone station-mapping
ARS Digit Conversion:	list ars digit-conversion

Command Category	Command Syntax
AAR Digit Conversion:	list aar digit-conversion
Traffic Measurements	list measurements attendant group list measurements attendant posit list measurements call-rate **OR (on newer switches)** list measurements call-rate total list measurements block pn last list measurements load-b total last list measurements tone-r summ last list measurements trunk-gr summ last list measurements occup summ list measurements ip dsp-resource summary last-hour (if available)

10.1 Appendix B

The result of compliance testing the InfoPlus Security Audit solution is attached in this appendix. Note: Blank pages in the report were intentionally omitted.

Produced For
Avaya Compliance Testing

Customer Number:
Reflecting PBX Information from: **6/26/2007**

DISCLAIMER

Bristol Capital, Inc. and its authorized distributors provide assistance to Avaya customers in reducing the risk of loss due to toll fraud and unauthorized access to PBX Services. However, Bristol Capital does not guarantee security nor warrant that any solution or product will stop toll fraud abuse or prevent unauthorized access. Bristol Capital does not assume liability for any losses due to breaches of security in a customer's system subsequent to any audit services provided by Bristol Capital and/or its authorized distributors.

The information contained in this document is based upon data retrieved remotely from a PBX system. Some of the information presented may be derived, in whole or in part, from this data. Inconsistent and/or incorrect programming of the PBX may cause these derivations to be inaccurate. For the sake of consistency in these reports, there may be cases in which a best-effort attempt is made to derive particular information based upon related data in the PBX. As the reporting facilities of the PBX's hardware and software improve, the enhanced data will lead to more accurate InfoPlus reports. Technical errors encountered during the remote transfer of data from the PBX may cause spurious results in the report. Bristol Capital, Inc. does not guarantee the accuracy of the information presented, although reasonable attempts have been and will continue to be made to ensure InfoPlus reports are as accurate as possible.

This report and the information contained herein is to be used only for the purposes intended. Any disclosure of the information contained herein to parties other than the subscriber of this service, or the organization whose information is represented, is strictly prohibited.

Communications Management with InfoPlus

Regardless of the size or type of organization, there are a few basic concerns of every communications manager. InfoPlus services help address those various concerns through its integrated suite of reports and analyses.

Inventory
Configuration
Performance
Security
Backup

Security – The increasing importance of communications security is met through the InfoPlus PBX Security Audit. The Security Audit is a comprehensive detailed analysis of system programming. Over 50 computerized analyses are performed listing the Description, the Security Concern and Finding of each of the analyses. All violations of established security measures are highlighted with sufficient information to rectify the violation. More than just cost avoidance, the InfoPlus PBX Security Audit will ensure your communications system is not supporting unauthorized use.

A next logical step in gaining additional control over your telecommunications resources might be an InfoPlus Traffic Study. Now that the Security Audit will help you block all unintended traffic, the Traffic Study will analyze intended traffic, ensuring the most effective yet efficient communications possible. Cost savings and/or service improving recommendations are clearly provided, easily justifying the study's cost.

Other services in the InfoPlus suite include:

Inventory – InfoPlus Site Survey
- Inventory of each of the major PBX hardware and software components
- "End-of-Life" analysis
- Access to database for Enterprise customers

Configuration – InfoPlus SourceBook
- Details a PBX system's programming
- Graphics of each set and each button's feature or line assignment
- Lists of each defined group (Intercom, Call Pick-up, etc.)
- Clearly defines trunking, call routing and even Privilege Groups
- Service-improving Action Items are uniquely assembled for your system

Performance – InfoPlus Traffic Study
- Consultative Report, not a "data dump"
- Supported by graphical representation of the "important" data
- Looks at Networks, Trunks, Consoles and even Processors
- Clear recommendations supported by factual data

Backup – InfoPlus Backup Service
- Off-site backup of your PBX's configuration
- Available at any time for restoration through the internet

Please contact your telecommunications vendor for additional information about these services.

Table of Contents

Introduction

We are pleased to provide you with the following Security Audit to help you identify and address areas of concern involved with the security of your telecommunications system.

Security of telecommunications services often involves the striking of a fine balance between business needs and the restrictive programming of various system features. As a result, the report can not tell us whether there is in fact a misuse of communications services taking place, but rather points out those areas where, and under what circumstances, abuse could take place. It is also intended to make you aware of the more mundane aspects of security practices and procedures as they relate to your telecommunications system.

The majority of this report is necessarily of a technical nature as it addresses the programming of sophisticated computerized systems. As a consequence, the report contains some mnemonics and feature names which may be unfamiliar to you. At the end of the report is a glossary for your reference.

In the abstract, you would think that establishing calling privileges and capabilities would be rather straightforward. Unfortunately, as users and special services demanded more flexibility, a very interrelated set of features has been created. As such, care should be taken in making modifications as changes in one area may impact calling capabilities in another.

To derive the full benefits, this report should initially be reviewed with your vendor and/or in-house technical staff. During this review it is likely that several areas will require further internal investigation before making modifications. As such, a complete Security Audit process may require two reviews, with this document helping to focus attention on the more critical areas.

Conventions Used in This Report

This report contains a number of topics detailing a wide array of security issues, grouped into chapters of related topics. Each topic contains a Description section, which briefly describes the PBX feature(s) it analyzes, a Security Concerns section, which explains different ways the feature(s) and their settings could be exploited, and an Analysis section, a computerized examination of your system with respect to the options in question, complete with recommendations of how to make your system more secure, if applicable. Within the Analysis section, anything that we feel requires your further investigation is underlined and printed in red.

Definitions

Throughout the report, we make references to dialing sequences that could direct calls outside of your PBX network onto the public telephone network. We call these dialing sequences "external numbers" and define them as any sequence that is longer than seven digits or begins with an ARS Access code, AAR Access Code or Trunk Group Access Code.

References to area codes with high toll-abuse are based on the reports of the LincMad website as of November, 2001, and can be viewed at <http://www.lincmad.com/telesleaze.html>.

Passwords and Security Codes

There are several topics in this report that reference and/or analyze various passwords and security codes programmed in your PBX or related telecommunications equipment. For increased security, we do not display in this report the actual passwords, but rather only show the results of analyzing the password for sufficient complexity. Your telecommunications vendor will have the details needed to perform any of the recommended changes presented in this report.

1. Administrative Access

One of the most important aspects of PBX security is controlling the ability to change the programming of the switch. A PBX in which unauthorized users can make changes is equivalent to using no security measures at all. While the PBX does have some features to help control this administrative access, there are other points to consider. You must still guard both physical access to the switch and the passwords themselves. Managing password knowledge when employees change, and giving individuals only the access they require are also important. The following is an explanation of how the PBX helps you manage these administrative responsibilities.

1.1. External Security

Description

The first line of defense against remote access to your PBX may not be part of the PBX at all. Advanced modems can be used with your switch to provide an added layer of security. Modems can use one-time challenge/response combinations or require separate passwords be entered before any access to the PBX is granted.

Security Concerns

Use of a secure modem decreases the possibility that an unauthorized individual will gain access to your switch. It is recommended that such a device be used for increased security.

Analysis

You are currently using a secure modem.

Your secure modem Login Name is unacceptable for the following reason(s):

- Does not contain both alpha and numeric characters

1.2. NETCON Class Of Restriction (COR)

Description

NETCON data modules are used for administration of the PBX. Access to NETCON ports can be configured through the use of COR-to-COR restrictions.

Security Concerns

If NETCON ports are not properly restricted, it may be possible for an unauthorized individual to gain administrative access to your PBX by transferring to these ports and bypassing any external security devices (e.g., ASG Guard II/RPSD). To ensure proper restrictions, it is necessary to review the COR-to-COR restrictions of your Voice Mail COR especially. NETCON ports should be in their own unique COR.

Analysis

No NETCON ports were detected in your PBX.

1.3. Login Names and Passwords

Description

The data in your PBX can be modified and/or viewed using multiple Login Names and passwords. Each "Customer-Level" Login Name can be configured to allow manipulation of nearly 100% of your PBX's vital data. Close analysis of these settings should be conducted on a regular basis in order to ensure that only the necessary permissions are granted to each Login Name.

Security Concerns

Since they are the key to the main gate of the PBX, the Login Names and passwords should both be difficult to guess, protected as sensitive data, and changed frequently. You should never use default Login Names of 'bcms', 'browse', 'cust', 'nms' or 'rcust'. Customer Login Names should all be at least 7 characters long, use 90-day or less password aging, require ASG authentication, and should have at least 7-character passwords.

Analysis

Note: Manufacturer established Login Names such as "craft", "inads", "init", "cust", and any others which require higher access levels will not appear in this list. Please manually review the settings on these Login Names to ensure the highest security.

Access Security Gateway (ASG) is disabled in the Customer Options of this PBX, and the feature is unavailable to all Login Names. It is recommended that this option be enabled.

We were not granted permission to access this data. Please review the Login Names defined in your system for proper levels of security.

1.4. Login Privileges

Description

Each Login Name in your system can be assigned certain privileges and restrictions. It is important to only allow the level of access needed to each Login Name. For example, those Login Names used solely for administering stations should not have access to trunk administration or maintenance commands. Restrictions may also be put in place so that a technician who is only allowed to administer specific areas of the PBX cannot alter programming of other sensitive data (such as Vectors). Login Names with access to the INADs port are able to access the system remotely.

Security Concerns

Unique Login Names should be administered for specific purposes to allow for greater monitoring of system changes. Correctly restricting each Login Name for individual people accessing your PBX will increase security. Maintenance Login Names should be kept separate from administration Login Names and each Login Name's permissions should be reviewed on a regular basis to ensure that access is granted only to necessary commands. Access to the INADs port should only be granted to those Login Names which are to be used remotely. Turning this permission off for your local Login Names greatly increases your security.

Analysis

We were not granted permission to access this data. Please review the Login Names defined in your system for proper levels of security.

1.5. Invalid Login Security Violation Notification

Description

The PBX has the ability to alert you when an invalid login attempt is made. The threshold for the number of invalid login attempts (Login Threshold) within a certain time period (Time Interval) can be defined. Furthermore, each Login Name can be administered to be "locked out" after causing a Security Violation Notification.

Security Concerns

The combination of these features protects your PBX against password hacking. The simplest way to guess a password is to try all of the various combinations. The Security Violation Notification (SVN) feature makes this process unattractive by limiting the "guesses" that can be made in a given time period, as well as alerting on-site personnel to the hacking activity detected. Avaya recommends administering a notification threshold of 5 invalid login attempts in a 3 minute time interval. When using SVN, it is important to make sure the Referral Destination is being monitored regularly by appropriate personnel.

Analysis

Your PBX is not configured to use Invalid Login Security Violation Notification. It is strongly recommended that you administer this feature to warn you of hacking attempts.

1.6. Logoff Screen Notification

Description

There are two features that Avaya has deemed a security risk if left enabled - Facility Test Call and Remote Access. The logoff screen notification allows each user to be alerted if these features are enabled. Furthermore, an acknowledgment can be required in order to successfully logoff from the PBX. Facility Test Call allows stations to access trunks directly, bypassing certain restrictions. Remote Access allows incoming calls to receive "secondary dial-tone" and make outgoing calls. Both of these features are covered more in-depth in later sections of this document.

Security Concerns

Alerting technicians to the administration of Facility Test Call and Remote Access can greatly increase the security and lower the potential for abuse in your PBX. This notification can be used as a reminder that the features are to be removed when not in use, and can also alert the technician in the event that the features were enabled by an unauthorized individual.

Analysis

The following table displays the logoff screen notifications for your customer-level Login Names:

Login Name	Facility Test Call Notification	Remote Access Notification
We were not granted permission to access this data. Please review the Login Names defined in your system for proper levels of security.		

1.7. TTI Security Code Analysis

Description

Terminal Translation Initialization (TTI) is mainly used for relocating stations from one port in the PBX to another. An administrator or user may use a code to change the programming of a station.

Security Concerns

If your TTI security code is too simple or less than 4 digits, then a hacker may guess it and exploit the TTI feature. It is always recommended to change the TTI security code from the default to prevent this exploit.

Analysis

Terminal Translation Initialization (TTI) is enabled in both the Customer Options and System Features of your PBX. The feature is active, for additional security it is recommended that it be disabled if not required.

Your TTI Security code is unacceptable for the following reason(s):

- It is to easy to guess.

2. System Configuration

Certain aspects of your PBX's programming and configuration have system-wide influences. In this section, we present some of these high-level settings and recommend steps you can take to increase the overall security of your PBX.

Did you know?

While this section of the Security Audit will address certain high-level features of your system, an InfoPlus SourceBook may be ordered to gain a more complete understanding of the configuration of your system. The SourceBook answers many of the questions you may have about your system's configuration.

2.1. Software Version

Description

Avaya assigns a software version/release number for all enhancements that have been made since the introduction of the Definity G3 PBX platform.

Security Concerns

As with any software, problems and bugs found in older versions are fixed in later releases. In addition, features for improving the security of the PBX are often added over time. For these reasons, it is recommended to keep your software version current. Also, older software releases are no longer fully supported by Avaya, which can present problems when requiring assistance.

Analysis

Your current software version is R014x.00.0.730.5

2.2. I/O Devices

Description

Input/Output Devices are required for communication with the Avaya PBX. These devices can be either on-site (local) or at a remote location. The standard devices for communication include a TTY/VDT terminal and the INADS modem. Later releases of software also support communication with the PBX via Ethernet. A printer may also be connected directly to the PBX to keep hard-copies of system error messages, logs, and scheduled commands.

Security Concerns

The proper configuration of your Input/Output devices can help control access to the PBX and its programming. Using a printer to record system messages and logs is also recommended as a way to monitor suspicious remote activity.

Analysis

Customer Access to INADS port

We were unable to determine if Customer Access to the INADs port is enabled or disabled. Please review your INADs configuration to ensure the proper level of security.

The INADs port is used for remote administration and maintenance. Extensive security measures can be taken to ensure that this port is only accessed by authorized personnel. (See External Security section 1.1) By disabling access to the INADs port, you significantly decrease the chance of unauthorized access to the PBX. However, you will also relinquish the ability to use this port for remote administration and maintenance.

Printer Configuration

Your PBX is currently not configured to use a printer. Please configure a printer and ensure that it is working properly in order to effectively monitor your PBX.

2.3. Alarm Monitoring Configuration

Description

Avaya PBXs have the ability to record and alert you to warnings, errors and alarms, both minor and major, via the Operations Support System (OSS). The alarm-monitoring destination could be a telephone, modem, computer, or Voice Mail-related device.

Security Concerns

It is important to review the alarm monitoring configuration regularly. A PBX hacker may disable alarm monitoring to prevent alerting the customer to his activities. This can cause longer than necessary service outages. Be sure to test the alarm-monitoring device regularly to ensure that it is functioning properly.

Analysis

You have no OSS extension defined for alarm monitoring.

Alarm Origination is not activated. Please enable Alarm Origination to ensure a higher level of security.

2.4. Night Service Configuration

Description

Night Service allows incoming calls to be redirected to alternate endpoints when activated. Night Service is activated and deactivated by the use of a feature button on a console or station. Consoles, Trunk Groups, Hunt Groups, Tenants, and Listed Directory Numbers (LDN) can all have a Night Service redirection defined.

Security Concerns

A common method of communications abuse is to redirect calls to unauthorized external numbers. For most applications, your Night Service numbers should be internal extensions such as a Voice Mail system or a night bell. External numbers should be examined to ensure that calls are being sent to approved destinations. They should also be tested to ensure they provide the recommended far end disconnect supervision of Fast Busy (120 IPM) when the far end goes on hook and the calling party remains off hook.

Analysis

You have no Night Service extensions specified.

The following devices have the ability to activate and deactivate Night Service:

Extension	Equipment Type	Name
No devices with the ability to activate or deactivate Night Service were detected.		

3. Assessing and Measuring Abuse

An important part of a complete security regimen is to record and track the system access, software modifications, and traffic patterns of your PBX. An early warning sign of abuse is activity that does not conform to the typical patterns of your business. For example, calls being placed after-hours, or to unusual destinations could indicate improper use of the facilities. The topics in this section address several ways you can monitor your PBX activity. However, they are only the first part of assessing abuse. The data provided by these features must be checked regularly and compared against established norms to help control abuse.

3.1. History Log Configuration

Description

The PBX has the ability to store a log of system access and command execution, as well as other system-related messages. The history log is easily printed out or viewed on either a local or remote terminal. There are options to enable or disable certain history messages in later releases of software.

Security Concerns

You should review the PBX's history to monitor any unauthorized administrative access to the system, particularly during night hours. For maximum benefit, the history log should record all possible messages.

Analysis

Your PBX is currently configured to collect all possible messages.

3.2. ASG - History Analysis

Description

Newer releases of PBX software allow for ASG one-time challenge/response authentication to be used for individual Login Names. With this feature enabled, the PBX keeps a log of customer-level ASG logins.

Security Concerns

When a user logs in using ASG, a record of the login attempt is kept in the ASG history. Logins that fail to authenticate will show up as being rejected. Rejections can be the result of an invalid response to a challenge, an invalid password, or an expired Login Name. A high number of rejections is often an indication of unauthorized attempts to access your system's administration interface.

Analysis

The option for ASG Customer level logins is disabled. It is recommended that this option be enabled for added security.

3.3. Traffic Measurements

Description

The PBX allows you to track traffic measurements on Trunk Groups, thus enabling you to identify unexplained escalations in call volume, especially outside of normal operating hours.

Security Concerns

Avaya recommends you regularly review traffic measurements of various types, including unusually high peg counts, excessive numbers of long and short holding times, high usage of Route Patterns used for 0 + and 011 + calls, out-of-range busy hours of Trunk Groups, and the switch occupancy profile as compared to a typical 24-hour period.

Traffic Measurements

Your PBX is not currently measuring the following Trunk Groups hourly: 7-8. It is recommended that you enable hourly measurements for all Trunk Groups.

Did you know?

While this section of the Security Audit covers the security aspects of Traffic Measurement, an InfoPlus Traffic Study may be ordered to gain a more complete understanding of your organization's PBX traffic. The Traffic Study answers many of the questions you may have about your system's capacity to handle your needs.

3.5. Call Detail Recording (CDR)

Description

Call Detail Recording, or CDR, is a feature that captures key information for every call made in the system. This information includes such details as the time and duration of the call, the called/calling parties involved, and the Authorization Code used to place the call.

Security Concerns

Calls placed during off-hours, or to unusual locations, can indicate improper use of the PBX facilities. CDR should be used to monitor your calling patterns and establish norms against which you can compare future activity. However, since CDR records can include sensitive data, it is important to control their output. If a hard copy of the CDR is produced, it should be disposed of properly.

Analysis

CDR is currently configured to use CDR1 as the primary endpoint. Please verify that this is the correct destination and that collection is functioning properly.

You are currently suppressing CDR for ineffective call attempts. This is not the recommended setting and should be changed in the CDR System Parameters.

All Trunk Groups are currently generating CDR data. This is the recommended configuration.

Did you know?

InfoPlus CDR is a web-based Call Detail Recording service that removes the burden of system operation and management while delivering a selection of completed weekly or monthly reports to your desktop. The same web portal that delivered this report can satisfy many of your communications management needs.

4. Stations

Many of the calling capabilities that have significant impact on long-distance charges are defined with the Class of Restriction and Class of Service of your stations. Access to certain features depends upon both the station's configuration and its COR and COS assignments. In these cases, it's best to review all members in the COR/COS since the stations' configuration may change at any time, perhaps inadvertently. In this section we analyze several of these features and capabilities, and look for potential holes in your security setup.

Did you know?

While this section of the Security Audit will address the security aspects of stations, an InfoPlus SourceBook may be ordered to gain a more complete understanding of the configuration of your system. The SourceBook answers many of the questions you may have about your system's configuration.

4.1. Basic Access Restrictions

Description

This topic addresses two Class of Restriction settings that define the basic access restrictions for stations: Calling Party Restriction and Facility Restriction Level. Calling Party Restriction defines the overall access the station has to the public network (for example, can only place outgoing non-toll calls). The Facility Restriction Level is a further check that allows the station to only access facilities with an identical or lower FRL.

Security Concerns

Stations with a Calling Party Restriction of "none" or "tac-toll" are the least restricted and normally have access to the public network. Facility Restriction Levels range from 0, the most restrictive, to 7, the least restrictive. Stations with an FRL of 7 generally have more trunking facilities available to them, and should be reviewed to ensure the high FRL is necessary.

Analysis

Listed below are all CORs in your PBX with a Calling Party Restriction of "none" or "tac-toll" and/or which are assigned an FRL of 7. For each of these CORs, we list the stations belonging to it so a decision can easily be made whether the enhanced permissions are appropriate for the group.

COR: 17

Calling Party Restriction: outward
Facility Restriction Level: 7

The following stations are assigned to COR 17:

Extension	Name	Equipment Type
No stations are assigned to this COR.		

4.2. Restricted Call List (RCL)

Description

The Restricted Call List is a table of dialed numbers that are denied access. Once a COR is programmed to use the RCL, access to the numbers on the RCL will be blocked through AAR/ARS regardless of the COR's Facility Restriction Level (FRL).

Security Concerns

To help reduce toll-abuse, high-toll area codes and exchanges as well as popular paid-for service numbers can be placed on the Restricted Call List. CORs with the same FRL can have different calling capabilities based upon whether or not they use the Restricted Call List, thus providing a finer degree of control.

Analysis

Area Codes known for high toll-abuse which you may wish to add to your Restricted Call List include: 268, 473, 649, 664, 758, 767, 784, 809, 868, and 876. These are Caribbean destinations in which your organization may not conduct business regularly. In addition, you may want to deny 1010-XXX 'Equal Access' numbers, 1-900 paid services, and 1-800 carrier specific services (e.g., 1-800-CALL-ATT).

There are no entries programmed in the Restricted Call List. This list should be used to block specific numbers (i.e. high-toll exchanges) from being called by stations.

4.3. Service Observe Feature

Description

The Service Observe feature allows certain users the ability to monitor calls placed within the PBX. Users with access to the Service Observe feature may monitor calls placed to extensions, Vector Directory Numbers and Agent Login IDs.

Security Concerns

If toll-abuse is suspected, the Service Observe feature can be used to monitor suspicious calls. Observers may use "listen" or "listen and talk" mode when monitoring calls. Optionally, a warning tone may be generated and heard by all listeners when a call is being monitored. It is recommended that you check with your local, state and federal laws to determine if the warning tone option must be enabled. Due to the nature of this feature and its potential for abuse, it is recommended to carefully and regularly review the users who have access to it. If the feature is not needed by your organization, it is recommended the two Feature Access Codes associated with it are left blank.

Analysis

Below is a list of the settings in your PBX related to Service Observing. It is recommended that the Service Observing related Feature Access Codes be left blank unless required by your business. Check with your local, state, and federal authorities to determine the legalities surrounding the Service Observe tone options.

Service Observing Warning Tone Enabled: N
Service Observing Conference Tone Enabled: N
Service Observing Allowed with Exclusion: N
Service Observing Listen Only Access Code: 127
Service Observing Listen and Talk Access Code: 128

The following is a list of stations which have a Service Observe button assigned:

Extension	Name	Type
There are no stations with a Service Observe button assigned.		

There are no Classes of Restriction configured to allow the Service Observe capability.

4.4. Station Features

Description

This topic addresses three powerful features of stations - Trunk-to-Trunk Transfer, Console Permissions, and Data Privacy. Trunk-to-Trunk Transfer allows an incoming call to be automatically redirected to an outbound trunk. Console Permissions allow a station to change the Facility Restriction Level (FRL) of other stations, thus altering their calling permissions. Data Privacy prevents analog data calls from being interrupted by attendant intrusion or features such as call waiting.

Security Concerns

The use of most of these features is a business and personnel decision. For example, Trunk-to-Trunk Transfer may allow unsupervised conference calls in which a user can conference in two long-distance parties, and then drop out of the conversation leaving them conferenced. This is not the recommended setting due to its abuse potential. It is also recommended to disable Trunk-to-Trunk Transfer Override, which can bypass COR-to-COR restrictions during a transfer, if it is not required. Console Permissions should only be given to sets which require the ability to change FRL levels and should not be located in publicly-accessible areas. Finally, it is recommended the Data Privacy feature only be enabled on modems, fax machines, credit card authorization devices, and other data terminals which require it.

Analysis

All Trunk-to-Trunk transfers are allowed in your feature-related system-parameters. This is not the recommended configuration and this feature should be disabled if not neccesary to business operations.

Listed below are all COSs in your PBX with Console Permissions, Data Privacy, or Trunk-to-Trunk Transfer Override enabled. For each of these COSs, we list the stations belonging to it so a decision can easily be made whether the enhanced permissions are appropriate for the group.

COS: 1

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 1:

Extension	Name	Equipment Type
60201	S8500-IP	9650
60202	On-8500	9610
62201	G150 Set 1	2500
62202	G150 Set 2	2500
62203	G150 Set 3	2500
62204	G150 Set 4	2500
64201	G250-IP96xx	9630
64202	G250-IP46xx	4620
64203	G250-Anal-1	2500

Extension	Name	Equipment Type
64204	G250-Anal-2	2500

COS: 5

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 5:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

COS: 6

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 6:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

COS: 7

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 7:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

COS: 8

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 8:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

COS: 13

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 13:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

COS: 14

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 14:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

COS: 15

Console Permissions are disabled for this COS, as recommended.

Data Privacy is enabled for this COS.

Trunk-to-Trunk Transfer Override is disabled for this COS, as recommended.

The following stations are assigned to COS 15:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

4.5. Call Forward Capabilities

Description

In the Avaya PBX, the Classes of Service control access to various Call Forwarding Features. These features include Call Forward (Busy/DA, All), Extended Call Forward (Busy/DA, All) and Call Forward Off-Net.

Security Concerns

While there are valid reasons to forward a phone, it is recommended that you review which stations have call forwarding capabilities. While it is commonly acceptable to allow normal Call Forwarding capabilities, only telecommuters should have access to the Extended Call Forward feature. Due to its abuse potential, Call Forward Off-Net should always be restricted unless there is a valid need to implement it in your PBX.

Analysis

Listed below are all COSs in your PBX with Call Forward All Calls, Call Forward Busy/DA, Extended Call Forward Busy/DA, or Extended Call Forward All Calls enabled. COSs with Restrict Call Forward Off-Net disabled will also be displayed. For each of these COSs, we list the stations belonging to it so a decision can easily be made whether the enhanced permissions are appropriate for the group.

Class of Service: 1

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 1:

Extension	Name	Equipment Type
60201	S8500-IP	9650
60202	On-8500	9610
62201	G150 Set 1	2500
62202	G150 Set 2	2500
62203	G150 Set 3	2500
62204	G150 Set 4	2500
64201	G250-IP96xx	9630
64202	G250-IP46xx	4620
64203	G250-Anal-1	2500
64204	G250-Anal-2	2500

Class of Service: 3

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 3:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

Class of Service: 4

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 4:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

Class of Service: 7

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 7:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

Class of Service: 8

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 8:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

Class of Service: 11

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 11:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

Class of Service: 12

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 12:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

Class of Service: 15

Call Forward All Calls: Enabled
Call Forward Busy/DA: Disabled
Extended Call Forward Busy/DA: Disabled
Extended Call Forward All Calls: Disabled
Restrict Call Forward Off-Net: Enabled

The following stations are assigned to COS 15:

Extension	Name	Equipment Type
No stations are assigned to this COS.		

4.6. External References

Description

Several redirection numbers on a station can be defined to go to numbers external to the PBX. Usually this incurs long-distance charges, and should be monitored for inappropriate use. In this topic we examine these redirection numbers and highlight those that appear to route a call outside the PBX. We look at all of a station's coverage points, as well as any currently forwarded destination.

Security Concerns

External redirection numbers should be checked to ensure they have an appropriate business need. Certain uses are common, such as an external Voice Mail system. Abuses occur when individuals forward their phone for personal use.

Analysis

The following tables lists stations whose various redirection destinations appear to be external. The destinations in question are listed under each category:

- Coverage Points (CP1 - CP6 columns)
- Call Forward Destination

The following extensions use a Coverage Path containing one or more Remote Coverage Points. For each entry, we show the actual number dialed with the Remote Coverage Point in parentheses.

Extension	Cov. Path #	CP1	CP2	CP3	CP4	CP5	CP6
No external Coverage Point references detected.							

The following extensions have a Call Forwarding destination assigned that appears to be external:

Extension	Name	Forwarded Destination
No Forwarded Destinations appear to be external.		

5. Trunking

Together with your stations, your trunking configuration defines the calling abilities of your users. It is important to manage your trunks and organize them by expense and/or business needs. Certain settings on trunks and Trunk Groups should be avoided to help you maintain a secure switch. In this section, we're going to analyze your Trunk Groups, trunks, and other trunking configuration issues.

Did you know?

While this section of the Security Audit will address the security aspects of trunks, an InfoPlus SourceBook may be ordered to gain a more complete understanding of the configuration of your system. For example, the Trunk Groups section of the SourceBook will clearly present exactly which Trunk Groups are used in the placing of outgoing calls and the order in which they are used. The SourceBook answers many of the questions you may have about your system's configuration.

5.1. Trunk Groups and Members

Description

Your trunks should be organized functionally into Trunk Groups. By definition, all of the trunks in a Trunk Group are of the same type and function. In the PBX, each Trunk Group has its own configuration. Like most of the PBX programming, there are certain settings at the Trunk Group level that could leave them vulnerable to abuse. We'll investigate those settings in this topic.

Security Concerns

There are many potential pitfalls to avoid when defining Trunk Groups. Something as simple as allowing outgoing calls on a Trunk Group that is supposed to be incoming only could be a security problem. Another common issue is enabling 'dial access' to a Trunk Group, and then defining a short or simple Trunk Access Code. It is recommended that all Trunk Access Codes be 4 digits long and non-trivial. If possible, 'dial access' to the Trunk Group should be disabled and all calls routed through ARS for increased security. Assigning a Trunk Group an FRL of 7 when a lower value would suffice is another sign of a poor security implementation. If an incoming destination is defined for a Trunk Group, it is recommended the number be verified, especially if it's an external destination. Other problems include failing to collect Call Detail Recording data for all Trunk Groups and incorrectly configured Classes of Restriction (COR). It is recommended that the CORs assigned to Trunk Groups are not used for other resources (e.g., stations) so that a robust COR-to-COR restriction plan can be defined. Finally, it is recommended that Automatic Circuit Assurance (ACA) is enabled for your Trunk Groups to help warn you about extremely short or long holding times which may be an indication of unauthorized activity.

The trunks themselves can pose their own security issues. We'll be checking specifically for trunks that have Night Service extensions programmed, as this represents a substantial risk to your PBX's security. All Night Service destinations should be verified, especially if the number is external to the PBX.

Analysis

Below is a list of all of the Trunk Groups in your PBX. Any items which do not agree with the Security Concerns are highlighted for review.

Trunk Group: 7

The following security-related items are part of the configuration for Trunk Group 7:

Trunk Group Name: PRI- 2 outside
Trunk Group Type: isdn
Trunk Group Direction: two-way
Incoming Destination:
Trunk Access Code (TAC): 1007
Dial Access: Disabled
Class of Restriction (COR): 1
Facility Restriction Level (FRL): 0
Call Detail Recording: Enabled
Automatic Circuit Assurance: Disabled

COR 1 is not unique to Trunk Groups.

The following Station CORs are not restricted from calling this Trunk Group's COR: 1. You should disable calling directly from station CORs to Trunk Group CORs to prevent users from bypassing ARS.

Trunk Group: 8

The following security-related items are part of the configuration for Trunk Group 8:

Trunk Group Name: IPTrunk to G350
Trunk Group Type: isdn
Trunk Group Direction: two-way
Incoming Destination:
Trunk Access Code (TAC): 1008
Dial Access: Enabled
Class of Restriction (COR): 1
Facility Restriction Level (FRL): 0
Call Detail Recording: Enabled
Automatic Circuit Assurance: Disabled

COR 1 is not unique to Trunk Groups.

The following Station CORs are not restricted from calling this Trunk Group's COR: 1. You should disable calling directly from station CORs to Trunk Group CORs to prevent users from bypassing ARS.

5.2. Direct Trunk Access

Description

Users can be given the ability to bypass the ARS least-cost routing feature and dial Trunk Access Codes directly. If the COR-to-COR restriction table does not restrict a station's COR from accessing a particular Trunk Group's COR, and the Trunk Group has the 'dial access' feature enabled, then direct access of the Trunk Group is possible from the station. This disables all of the security features built into the ARS design. Once a Trunk Group is accessed directly, the Calling Party Restrictions of the station's COR will be used to determine whether a particular call is allowed.

Security Concerns

When combined with a Calling Party Restriction of "none", "tac-toll" or "all-toll", directly accessing a Trunk Group gives users the full capabilities of the public network. This includes the ability to place any toll call including international numbers. With a Calling Party Restriction of "outward" the user is restricted to directly accessing only TIE Trunk Groups, but still has the ability to dial any string of digits including international, high-toll and long distance destinations.

Analysis

No CORs have Direct Trunk Access.

6. Controlling Calling Privileges

The configuration of your stations and trunks define basic access restrictions within the PBX. However, there are many other ways to modify these restrictions with various features and services. This section presents these features and addresses the configuration of each one individually. Some features further limit the capabilities of a station or trunk, while others circumvent restrictions already in place. Their intelligent use allows you to design a telecommunications solution that provides only the necessary functionality without opening the doors to unauthorized use.

6.1. System Abbreviated Dialing List

Description

The System Abbreviated Dialing List (also referred to as "Speed Call") allows users to place internal or external calls to predefined numbers by dialing a 2-digit code. The System Abbreviated Dialing List can store up to 100 entries with up to 24 digits each.

Security Concerns

Because a privileged System Abbreviated Dialing List can override the Class of Restriction (COR) of stations, it is important to verify the numbers stored in the list are approved destinations.

Analysis

There is no "system" Abbreviated Dialing List.

6.2. Group Abbreviated Dialing Lists

Description

The Group Abbreviated Dialing Lists (also referred to as "Speed Call" lists) allow users to place internal or external calls to predefined numbers by dialing a 2-digit code. The PBX is capable of having up to 100 different lists programmed. Each Group Abbreviated Dialing List can store up to 100 entries with up to 24 digits each.

Security Concerns

Because privileged Group Abbreviated Dialing Lists can override the Class of Restriction (COR) of stations, it is important to verify the numbers stored in the list are approved destinations. It is also important to control the individuals who can modify these lists.

Analysis

You have no Group Abbreviated Dialing Lists defined.

6.3. Authorization Codes

Description

Stations and trunks originating calls can use Authorization Codes to alter their Facility Restriction Level (FRL). Each Authorization Code is mapped to a COR and the caller assumes that COR's FRL when entered.

Security Concerns

Security Violation Notification (SVN) for Authorization Codes should be enabled when Authorization Codes are in use. It is recommended to use an SVN threshold of 10 or fewer invalid attempts in 3 or more minutes, and to ensure the Referral Destination is being monitored regularly by appropriate personnel. Authorization Codes that contain less than 7 digits or are simple to guess are not recommended since they don't provide adequate security for the enhanced privileges they provide. Those codes assigned to CORs with high FRLs and low Calling Party Restrictions can also present a possible security problem if not managed carefully.

Analysis

Authorization Codes are disabled in the Customer Options of your PBX, and disabled in System Features. The Authorization Code feature is disabled, and SVN for Authorization Codes is also disabled. It is recommended that SVN for Authorization codes be enabled in case this feature is used in the future.

Authorization Codes Security Violation Notification: Disabled

The following table lists all Authorization Codes in the PBX. The highlighted codes have failed one or more of the following checks:

- Contains a run of three or more consecutive digits
- Contains a run of three or more identical digits
- Is fewer than 7 characters long
- Code is assigned to a COR with an FRL of 6 or greater
- Code is assigned to a COR with a Calling Party Restriction of "none"

Authorization Code	COR	FRL	CPR = "none"
No authorization codes are programmed in your PBX.			

6.4. Account Codes

Description

The PBX can be configured to use CDR Account Codes for calls placed on the Toll List. The system administrator can configure the number of digits (1 to 15) that must be dialed within a certain time, and if the proper number of digits are not dialed, the call will not complete. The specific digits dialed are not verified in any way, only the number of digits must be correct. This feature is often used to associate an identifier (e.g., an account number) with calls for billing purposes.

Security Concerns

Requiring Account Codes for toll calls can offer a modest level of security against unauthorized users, and provide an additional means of tracking PBX usage. These codes will show up in CDR records and can assist you in recognizing toll-abuse.

Analysis

Your CDR configuration is currently configured to force entry of Account Codes, however no CORs are configured to use this feature. Configuring your CORs to force entry of Account Codes gives you an additional means of tracking PBX usage.

7. Controlling Feature Access

Avaya PBXs have many calling features, which if not properly controlled could allow unauthorized users to commit toll fraud. Many of these features can be activated or deactivated at any station, or even through Voice Mail ports. Access to several of these features can be controlled by settings within the Class of Service, while others may be disabled altogether.

7.1. Feature Access Codes

Description

Feature Access Codes (FAC) are user-defined numbers of up to four digits which can be used to activate and deactivate certain features within the PBX. When a code is not defined, the associated feature is generally inaccessible.

Security Concerns

Feature Access Codes for features with security implications should not be accessible through Voice Mail. Ensure that the digits of these Feature Access Codes are blocked in the Voice Mail system, or translated to an extension, attendant, announcement or disconnect - never to the Feature Access Code itself. It is recommended that you leave the Feature Access Code empty for any features that are not required by your organization, as a measure to prevent inappropriate use.

Analysis

AAR/ARS/ISDN Feature Access Codes

Ensure that the following digits are blocked or intercepted from your Voice Mail system:

Feature Name	Feature Access Code
AAR	*08
ARS - Access Code 1	*99
ARS - Access Code 2	#99
ISDN Access Code	Blank

Critical Feature Access Codes

The following Feature Access Codes have security implications and should be blocked in your Voice Mail system. If it is not necessary to have them enabled, their Feature Access Code should be left blank.

Feature Name	Feature Access Code
Abbreviated Dialing - List 1	*01
Abbreviated Dialing - List 2	*02
Abbreviated Dialing - List 3	*03
Call Forward Activation - Busy/DA	#11
Call Forward Activation - All	*10
Change Coverage	*13
Data Origination	*15
Data Privacy	*16
Facility Test Call[†]	*22
Personal Station Access Associate	*32
Personal Station Access Dissociate	Blank
Station Security Code Change	*41

[†]The Facility Test Call code should only be enabled when in use. After testing is complete, Avaya recommends removing the access code from the PBX in order to increase security.

7.2. Station Security Codes

Description

Station Security Codes (SSC) are used with several features, including Station Lock, Personal Station Access (PSA) and User Administration of Redirected Calls. In order to use these features, the Station Security Code for the particular station must be entered.

Security Concerns

Short or simple Station Security Codes may not provide adequate security. It is recommended the minimum length of Station Security Codes be set to at least 4. Any station that does not require the use of the features protected by a Station Security Code should not have one defined. You can prevent users from changing the Station Security Code by removing the Feature Access Code for 'Station Security Code Change Access Code'. Security Violation Notifications for Station Security Codes should be enabled when available in later Avaya software. It is recommended to use an SVN threshold of 10 or fewer invalid attempts in 3 or more minutes, and to ensure the Referral Destination is being monitored regularly by appropriate personnel.

Analysis

Station Security Codes Security Violation Notification: Disabled

The minimum security code length is 4. This is acceptably complex.

There are 8 stations in your PBX with a Station Security Code currently defined. The Station Security Code Change option is enabled in your Feature Access Codes, allowing a user to alter their existing code at any time.

The following stations in your PBX have Station Security Codes assigned:

Extension	Name	Equipment Type
60201	S8500-IP	9650
60202	On-8500	9610
62201	G150 Set 1	2500
62202	G150 Set 2	2500
62203	G150 Set 3	2500
62204	G150 Set 4	2500
64201	G250-IP96xx	9630
64202	G250-IP46xx	4620

7.3. Modems and Faxes

Description

Avaya recommends reviewing the capabilities of ports configured for fax machines and modems, to ensure that they are not using features which may be exploited.

Security Concerns

Certain types of fax machines, modems and answering machines respond to specific tones presented to them, sometimes allowing dial tone to be returned to the caller. Upon receiving dial tone from the PBX, the caller is free to dial any number allowed by the COR of the fax machine or modem. In order to ensure that these ports are protected from this sort of exploitation, Avaya recommends disabling the Switch Hook Flash and Distinctive Audible Alert features in the station programming.

Analysis

Below is a list of all stations identified as possible security risks. These stations all have "FAX", "FX", or "MOD" in their name, or the station type is aliased to "modem" or "fax", and meet one of the following additional criteria:

- Distinctive Audible Alert is enabled
- Switch Hook Flash is enabled

Please note that it is possible for some modems or faxes in your PBX to be missed by this test, or for stations which are neither a modem nor a fax machine to be detected. While the following list can act as a guideline, it is recommended that you review your stations in depth.

Extension	Name	COR	Switch Hook Flash	Distinctive Audible Alert
No modems or faxes matching above criteria were detected.				

8. Remote Access

This section addresses Remote Access, a very powerful feature that if not properly controlled could open your PBX to abuse by external callers. This feature requires special consideration. Although the feature is part of the standard PBX configuration, it can and should be disabled system wide upon initial installation if not required for your business.

8.1. Remote Access Feature (DISA)

Description

The Remote Access feature, sometimes referred to as Direct Inward System Access or DISA, allows a user to dial an extension in the PBX and receive secondary dial-tone. Depending on the configuration, the user may then dial internal or external numbers as if they were using a station in the PBX. This feature is often used by businesses where employees are traveling regularly and need to place business-related calls from outside the office.

Security Concerns

Remote Access, even when properly configured, can open the PBX to toll-abuse from the public network. If it is not required, removing this feature from the PBX software provides the greatest security. If Remote Access is required, it should be heavily protected through the use of Authorization Codes, Barrier Codes and tight access restrictions. It is recommended that Security Violation Notifications for Remote Access be enabled if this feature is in use, and that the SVN system disable the Remote Access feature upon the thresholds being reached. You should define an SVN threshold of 10 or fewer invalid attempts in 3 or more minutes, and ensure the Referral Destination is being monitored regularly by appropriate personnel. In addition, Remote Access dial-in numbers should not be published, and their distribution should be limited to employees who require the feature.

Analysis

Remote Access is not enabled in your PBX, although is still can be. If you do not have a need to use this feature, then it is recommended that you permanently disable it in your PBX.

Remote Access Security Violation Notification: Disabled

8.2. Barrier Codes

Description

For additional security, Remote Access should be assigned Barrier Codes that must be entered before the user gains access to secondary dial-tone. These codes can be 4 to 7 digits in length and are assigned to a specific COR, Tenant and COS. They can also be assigned a maximum number of calls and an expiration date to limit their use.

Security Concerns

Barrier Codes that are easy to guess should not be used. They should all be at least 6 digits in length, although 7 is always preferred. If the Barrier Code length is left blank, then no Barrier Codes are required for secondary dial-tone, significantly lowering the security of the Remote Access feature. The Class of Restriction and Class of Service assigned to each Barrier Code should be fairly restrictive to ensure that remote users are only able to dial necessary numbers. If applicable, a low number of maximum calls should be specified, as well as an expiration date less than 1 month from the date the Barrier Code was created.

Analysis

Barrier Code length is not defined in your PBX, disabling the required use of Barrier Codes for the Remote Access feature. It is recommended that you define a length of at least 6 digits, or permanently disable Remote Access if it is not required.

Below is a list of every Barrier Code programmed in your PBX and its associated programming. Potential security risks have been highlighted in red and underlined. Remote Access programming should be reviewed on a regular basis and should be permanently disabled if not necessary to your business.

Barrier Code	COR	TN	COS	Expiration Date	No. of Calls	Calls Used
No Barrier Codes defined.						

9. Call Routing

In addition to the restrictions placed at the station or trunk level, it's important to control how both incoming and outgoing calls are routed through the PBX network. We'll be analyzing the various features of Avaya's Alternate Route Selection (ARS) feature, looking for unusual routing configurations. Incorrect routing could prevent certain calls from being placed or received at all, or could send calls over unnecessarily expensive trunking facilities. The routing configuration is also used to supplement the definition of individual calling restrictions, defining who can call where and at what times.

9.1. Route Patterns

Description

For each network call translated in an Avaya PBX, ARS or AAR selects a Trunk Group from a list of possible outgoing Trunk Groups to complete the call. The list of possible Trunk Groups to a particular destination is called a Route Pattern, and each Trunk Group specified in the pattern is given a preference. Typically, the first preference in a Route Pattern should be the least expensive Trunk Group to a destination, and the remaining Trunk Groups in the list are more expensive.

Security Concerns

Each Route Pattern preference may both delete and insert digits. These digits should be carefully examined for any strange redirection of calls. Assigning an entry in a Route Pattern an FRL of 0 should be limited, as this permits all other resources to access it.

Analysis

The following table presents a list of all Route Patterns and preferences, as well as their associated FRL values. Low FRLs should be reviewed and increased if necessary.

Route Pattern	Preference	FRL
8	1	0

9.2. Alternate FRL

Description

The Avaya PBX can allow stations and trunks to use an alternate (and usually less-restrictive) FRL when necessary to modify their calling permissions. This feature is activated and deactivated by the console.

Security Concerns

If an Alternate FRL is assigned incorrectly, certain stations and trunks may not be as restricted as they would appear if you analyzed only the FRL of their associated CORs. Vice versa, an Alternate FRL that is too restrictive may hinder a station or trunk from being able to place calls as needed.

Analysis

The following presents a list of your FRLs (0-7) and their associated Alternate FRL. If the Alternate FRL allows greater access, it will be highlighted for review.

FRL	Alternate FRL
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

None of your FRLs are currently affected by the Alternate FRL feature.

9.3. Time of Day Routing

Time of Day Routing

Time of Day Routing can be used to alter a station's calling abilities based on both the time of day and day of the week. This feature is normally used to restrict long distance access after business hours.

Security Concerns

Since Time of Day Routing changes which Route Patterns are used when dialing through AAR/ARS, it is important to ensure that access to long distance and international destinations is properly restricted. Any off-hours configuration granting long distance or international access should be reviewed.

Analysis

Time of Day Routing Plan: 1

Time of Day 1 is not in use by any CORs.

0 stations are assigned to this plan.

Time Period	CORs with Long Distance Access	CORs with International Access
No Time of Day Configuration for this plan.		

Time of Day Routing Plan: 2

Time of Day 2 is not in use by any CORs.

0 stations are assigned to this plan.

Time Period	CORs with Long Distance Access	CORs with International Access
No Time of Day Configuration for this plan.		

Time of Day Routing Plan: 3

Time of Day 3 is not in use by any CORs.

0 stations are assigned to this plan.

Time Period	CORs with Long Distance Access	CORs with International Access
No Time of Day Configuration for this plan.		

Time of Day Routing Plan: 4

Time of Day 4 is not in use by any CORs.

0 stations are assigned to this plan.

Time Period	CORs with Long Distance Access	CORs with International Access
No Time of Day Configuration for this plan.		

Time of Day Routing Plan: 5

Time of Day 5 is not in use by any CORs.

0 stations are assigned to this plan.

Time Period	CORs with Long Distance Access	CORs with International Access
No Time of Day Configuration for this plan.		

Time of Day Routing Plan: 6

Time of Day 6 is not in use by any CORs.

0 stations are assigned to this plan.

Time Period	CORs with Long Distance Access	CORs with International Access
No Time of Day Configuration for this plan.		

Time of Day Routing Plan: 7

Time of Day 7 is not in use by any CORs.

0 stations are assigned to this plan.

Time Period	CORs with Long Distance Access	CORs with International Access
No Time of Day Configuration for this plan.		

Time of Day Routing Plan: 8

Time of Day 8 is not in use by any CORs.

0 stations are assigned to this plan.

Time Period	CORs with Long Distance Access	CORs with International Access
No Time of Day Configuration for this plan.		

9.4. Digit Manipulation

Description

AAR, ARS as well as Each Route Pattern in the PBX can optionally define a number of digits to delete from a dialed sequence, and/or a digit sequence to insert. Digits are deleted from the beginning of the sequence that was dialed, and the new digits may be added in their place potentially changing the call's destination after it has passed through AAR/ARS. This can be used to route specific calls to a different location than they would normally go, such as routing a call over a TIE line to another office where the call would be local. Digit Manipulation can also be used to add outpulsed digits that may be required by the central office for certain call types.

Security Concerns

Digit Manipulation is a feature that can easily be exploited to make calls that would otherwise be denied by a properly configured AAR/ARS table. Since digits are deleted and inserted from the beginning of the sequence that is dialed, it would be an easy matter for someone to create a Route Pattern that replaces whatever area code was dialed with, for example, a 1-900 number. This Route Pattern could be assigned to an otherwise unused, innocuous looking AAR/ARS entry and allow fraudulent calls to be placed.

Another, more difficult to detect approach to fraud would be the creation of a Digit Manipulation entry which results in an extremely short dialed sequence. Once the call routes using this entry, few or no digits will be outpulsed to the Trunk, which may then wait for more digits. The caller can then enter more digits from their keypad, potentially allowing them to make calls that bypass AAR/ARS rules for both entries and sequence length.

Analysis

The following tables list all of the AAR/ARS entries in your PBX for which the high-level AAR/ARS digit manipulations are applied. For each entry, we list the number of digits that are deleted, the digits which are inserted and an example of what the entry would become after manipulation. All manipulated sequences should be checked for accuracy to ensure calls are being routed as expected. We highlight those entries which can result in fewer than three outpulsed digits, as these entries can be exploited by users dialing extra digits after the AAR/ARS analysis.

AAR Table Manipulations

Entry	# Deleted Digits	Inserted Digits	Becomes	Min Length	Analysis
x11	0		x11	3	
1	0		1	4	
0	0		0	1	Fewer than 3 digits

ARS Table Manipulations

Entry	# Deleted Digits	Inserted Digits	Becomes	Min Length	Analysis
No digit conversions were detected in your ARS Digit Conversion table.					

The following tables list all the AAR/ARS entries in your PBX which ultimately point to Route Patterns that perform digit manipulation. For each entry, we list the number of digits that are deleted, the digits which are inserted, an example of what the entry would become after manipulation, and the the fewest number of digits that can result

from the entry. All manipulated sequences should be checked for accuracy to ensure calls are being routed as expected. We highlight those entries which can result in fewer than three outpulsed digits, as these entries can be exploited by users dialing extra digits after the AAR/ARS analysis.

AAR Route Pattern Manipulations

Entry	Route Pattern	Pref	# Deleted Digits	Inserted Digits	Becomes	Min Length	Analysis
3	8	1	1	-		5	

ARS Route Pattern Manipulations

Entry	Route Pattern	Pref	# Deleted Digits	Inserted Digits	Becomes	Min Length	Analysis
No digit manipulations were detected in any Route Patterns used by your ARS tables.							

Unused Route Patterns

The following Route Patterns do not appear to be in use by your AAR/ARS system. Those which define digit manipulations are highlighted. It is recommended that you review these Route Patterns and consider deleting any that will not be used.

Route Pattern	Pref	FRL	# Deleted Digits	Inserted Digits
No unused Route Patterns detected in your PBX.				

9.5. High Toll Calling

Description

The AAR/ARS tables determine which Route Pattern is used to route calls to particular locations. Each area code or local exchange is assigned a Route Pattern or Partition Group that defines the Trunk Groups available for calls to that particular destination. Each entry within the AAR/ARS tables has a maximum and minimum number of digits expected.

Security Concerns

It is critical to make sure calls such as 1-900 pay services, area codes known for their high toll abuse (i.e. 809), and international area codes be properly restricted in your AAR/ARS configuration. Other translation table entries that should be monitored include the 976 exchange, international access codes, "Equal Access" codes, and 1-800 carrier specific services. Entries for international (011) and operator assisted (0) calls should specify an appropriate minimum and maximum expected length to prevent users from truncating CDR records by pausing during the dialing sequence. It is possible to inadvertently allow calls to numbers you intend to restrict through the inclusion of higher-priority entries, especially involving the use of the wildcard character 'x', so every rule that is added to the AAR/ARS tables should be inspected for possible side-effects.

Even with appropriate and sufficient AAR/ARS tables, toll fraud can still be achieved through misconfiguration of the Digit Manipulation feature of the Route Patterns. Please refer to the Digit Manipulation section for details on this feature.

Analysis

Foreign Area Codes

Your PBX appears to restrict all Foreign Area Codes.

High Toll/Fraud Area Codes and Exchanges

Your PBX appears to restrict all High Toll/High Fraud Area Codes and Exchanges.

9.6. International Calling

Description

If programmed correctly, the ARS system can handle directly dialed international numbers (those beginning with 011) just like any other long-distance number. A user's or trunk's COR indirectly determines whether international dialing is allowed through ARS.

Security Concerns

The high expense of international calls is the primary reason to restrict this capability to only those users who require it. If your organization does not have a need to regularly call internationally, you should consider requiring an Authorization Code to place these calls. It is also recommended that the Route Patterns allowing international calls require an FRL greater than 0 on all entries to appropriately limit the resources that can use them. As this topic only addresses ARS dialing, you should also reference the Direct Trunk Access topic to investigate the ability to dial internationally without using ARS.

Analysis

There are no route patterns which allow access to international calls.

10. Voice Mail Ports (Audix)

The power and flexibility of modern Voice Mail applications make them a common target of hackers attempting to gain unauthorized access to a PBX. Because of this, the PBX interface to the Voice Mail system demands special scrutiny. The following sections analyze the configuration of this system's Audix Voice Mail ports to limit their vulnerability.

10.1. Voice Mail Ports Class of Restriction (COR)

Description

Avaya recommends that all Audix Voice Mail ports be configured with specific settings to increase the security of the application. By assigning specific COR settings, the ports can be restricted from calling out altogether, or be limited by your AAR/ARS configuration.

Security Concerns

If the outcalling feature of the Voice Mail is not needed, Avaya recommends configuring the COR with a Calling Party Restriction (CPR) of "outward". If outcalling is necessary, then it is recommended that you review your AAR/ARS configuration to ensure that is it limited as much as possible. Voice Mail ports with a high FRL are less restricted by AAR/ARS, so Avaya recommends an FRL assignment of 0. By restricting the COR of the Voice Mail ports from the COR of the Trunk Groups in your system (using COR-to-COR permissions), you can prevent the Voice Mail from calling a Trunk Access Code and providing external dialtone. For ease of administration and increased security, the Voice Mail ports should be assigned their own unique COR.

Analysis

No Voice Mail ports were detected.

10.2. Voice Mail Ports Class of Service (COS)

Description

Avaya recommends that all Audix Voice Mail ports be configured with specific settings to increase the security of the application. By assigning specific COS settings, the ports can be restricted from having certain high-risk features enabled.

Security Concerns

Avaya recommends that the Voice Mail ports be in their own unique Class of Service (COS). Call Forwarding for all Voice Mail ports should be disabled. Call Forwarding Off-Net should be restricted. Console Permissions, Data Privacy, and Trunk-to-Trunk Transfer Override should all be denied. By restricting these features, your Voice Mail ports are less likely to be used for toll fraud/abuse.

Analysis

No Voice Mail ports were detected.

10.3. Voice Mail Port Configuration

Description

Avaya recommends that all Audix Voice Mail ports be configured with "Switchhook Flash" enabled and "Distinctive Audible Alert" disabled.

Security Concerns

Unauthorized individuals have been known to exploit the misconfiguration of Voice Mail ports to return secondary dialtone, allowing them to make calls from your PBX.

It is especially important to disable Distinctive Audible Alert on any adjunct port (fax machines, Voice Mail, Voice Recognition ports) as these are the most common areas of attack and are not physically monitored by a person.

Analysis

No Voice Mail ports were detected.

11.1. Voice Recognition Ports Class of Restriction (COR)

Description

Avaya recommends that all Voice Recognition ports be configured with specific settings to increase the security of the application. By assigning specific COR settings, the ports can be restricted from calling out altogether, or be limited by your AAR/ARS configuration.

Security Concerns

If off-net calling for Voice Recognition ports is not needed, Avaya recommends configuring the COR with a Calling Party Restriction (CPR) of "outward". If off-net calling is necessary, then it is recommended that you review your AAR/ARS configuration to ensure that it is limited as much as possible. Voice Recognition ports with a high FRL are less restricted by AAR/ARS, so Avaya recommends an FRL assignment of 0. By restricting the COR of the Voice Recognition ports from the COR of the Trunk Groups in your system (using COR-to-COR permissions), you can prevent the Voice Recognition ports from calling a Trunk Access Code and providing external dialtone. For ease of administration and increased security, the Voice Recognition ports should be assigned their own unique COR.

Analysis

No Voice Recognition ports were detected.

11.2. Voice Recognition Ports Class Of Service (COS)

Description

Avaya recommends that all Voice Recognition ports be configured with specific settings to increase the security of the application. By assigning specific COS settings, the ports can be restricted from having certain high-risk features enabled.

Security Concerns

Avaya recommends that the Voice Recognition ports be in their own unique Class of Service (COS). Call Forwarding for all Voice Recognition ports should be disabled. Call Forwarding Off-Net should be restricted. Console Permissions, Data Privacy, and Trunk-to-Trunk Transfer Override should all be denied. By restricting these features, your Voice Recognition ports are less likely to be used for toll fraud/abuse.

Analysis

No Voice Recognition ports were detected.

11.3. Voice Recognition Port Configuration

Description

Avaya recommends that all Voice Recognition ports be configured with "Switchhook Flash" enabled and "Distinctive Audible Alert" disabled.

Security Concerns

Unauthorized individuals have been known to exploit the misconfiguration of Voice Recognition ports to return secondary dialtone, allowing them to make calls from your PBX.

It is especially important to disable Distinctive Audible Alert on any adjunct port (fax machines, Voice Mail, Voice Recognition ports) as these are the most common areas of attack and are not physically monitored by a person.

Analysis

No Voice Recognition ports were detected.

12. Vectors and Vector Directory Numbers

The following section analyzes various aspects of this system's Vectors and Vector Directory Numbers.

12.1. Vectors

Description

Vectors are a collection of steps used to handle the routing of calls. These steps can be used to collect digits from the caller and route the call to another destination.

Security Concerns

If not configured properly, a Vector could allow an unauthorized user to enter digits that establish an off-premise call. All Vectors with steps to collect digits and route calls should be reviewed to ensure that they are restricted as much as possible. Any Vector that includes a route-to step to an off-premise number should be checked to ensure the legitimacy of that number.

Analysis

No vectors were detected with "collect" or "route-to" steps.

12.2. Vector Directory Numbers Class Of Restriction (COR)

Description

Vector Directory Numbers (VDN) are "soft extensions" in the PBX that direct a call to a Vector. If the call is re-routed by the Vector, the call carries the Facility Restriction Level (FRL) and Calling Party Restrictions (CPR) of the VDN.

Security Concerns

You should assign the lowest possible FRL and most restrictive CPR (preferably "outward") to the COR used by VDNs. Facility Test Call should also be denied in the COR programming, as unauthorized users can possibly exploit the feature to generate calls without the restrictions or AAR/ARS. Avaya recommends that any CORs assigned to your VDNs are not used by other facilities (e.g., stations).

Analysis

No VDNs were detected in your PBX.

Viewing your Security Audit on the Web

Introduction

Every InfoPlus Security Audit that is run will be automatically archived and uploaded to our web site for secure online viewing. Each account is assigned a unique Web Code, and entering this code on our web site provides a list of all InfoPlus reports archived for the account, and the dates they were run. We will store every Security Audit for at least three years, allowing you to compare current information with previous audits. Also, this technology allows any number of your people, across town or across the country, to view the data simultaneously and discuss its implications.

Suggested Software

The Security Audits will be stored in PDF format, also known as Adobe Acrobat™ format. You will need the Adobe Reader application (version 5.0 or later) and any web browser to view the PDF files. Adobe Reader is free to download from Adobe's web site (www.adobe.com).

Instructions

Go to the InfoPlus web site located at www.infoplusonline.com. You'll need to enter the Web Code in the form on the home page. If you do not know the Web Code for this PBX, please contact your vendor representative. The code is case–sensitive, and may contain both numbers and letters. Once a correct code is entered, you will be presented with a list of all available InfoPlus reports for the account, along with the date of each report. Select the report you wish to view, and it will either be presented directly in your browser window, or within a new Adobe Reader™ window. Use the navigation bar to flip through the report page by page, or use the index at the left to access a particular section.

Additional Security Precautions

There are several other areas of concern, in addition to the programming of your PBX and Voice Mail, which must be addressed for a complete security audit. This appendix lists some additional, external sources of potential abuse or theft of telecommunications services which should be investigated.

Disconnect Supervision for External Calls

When calls are routed through your PBX to valid external destinations, such as a Night Service number, it is recommended to verify the disconnect supervision at the far end. If a call is routed to the external destination, the disconnect supervision at the far end will be either a fast busy signal (120 IPM), or a burst of dial tone. A burst of dial tone can enable the caller to seize the trunk by dialing any digit. To prohibit this form of toll fraud, request the far end disconnect supervision be changed from dial tone to fast busy (120 IPM). This request should be made to the far end local service provider.

Dumpster Diving

Any printed or electronic copy of data from your PBX or Voice Mail must be disposed of properly to prevent unauthorized individuals from using the data to perpetuate toll fraud or abuse. Documents that list passwords, Authorization Codes, Remote Access numbers, etc. are of particular importance, but any document exposing the programming of either the PBX or Voice Mail can be a potential security risk. Shredding paper documents or physically destroying any electronic media can help prevent this theft of information.

Employee Changes

Even if a snapshot of your telecommunications equipment programming shows no obvious signs of security problems, it is important to understand that this data operates in a dynamic environment and must be kept up to date. When employees leave the organization, it's vital to take a survey of their telecommunications resources and deactivate appropriate facilities. If they were assigned an Authorization Code, it should be removed from the switch and not reused. The Station Security Code, if assigned, should be removed or changed. Any voice mailboxes assigned to the user should be disabled or removed. Having a checklist for such situations may be helpful if they occur regularly.

IP Access

Modern PBXs have an additional means of communicating with the switch and performing administrative maintenance - through the Internet Protocol over your Local Area Network (LAN), and potentially the internet. If your switch has this ability, it is imperative that your network administrator restrict access to the PBX through the use of a hardware firewall. If this interface is not protected, it may allow any individual with internet access to attempt to login to the PBX. It is recommended to limit IP access to your local network, and only to authorized administrators on that network.

Glossary

Abbreviated Dialing
A feature providing station users access to system, group or personal lists allowing them to dial frequently called telephone numbers using a 1- to 3-digit code. System and Group lists may also be configured as 'privileged', thus overriding any restrictions placed on an extension.

Access Security Gateway (ASG)
A security system available to Avaya PBX systems which uses one-time challenge/response authentication and a hand-held ASG Key device to protect access to the administrative interface of the PBX.

Active (Coverage Paths)
A state where a user is on the phone and the instrument is capable of receiving another call on an additional call appearance button.

Audix
Avaya's Voice Mail platform for the Definity Call Servers.

Authorization Code
A code that a user may dial before placing a call to modify their Facility Restriction Level, usually to elevate their calling permissions. For example, you may require an Authorization Code before dialing international numbers to restrict their use.

Automatic Call Distribution (ACD)
A type of Hunt Group that presents incoming calls to multiple stations sequentially. These stations are called ACD Agents.

Automatic Circuit Assurance (ACA)
A feature which can monitor the holding times of trunk calls and notify personnel to unusually long or short call durations. This feature is often used to diagnose trunk malfunctions and highlight potential unauthorized use.

Automatic Route Selection (ARS)
A feature within the PBX which directs outbound calls to predefined Trunk Groups dependent upon the digits that were dialed.

Call Detail Recording (CDR)
A feature allowing the recording of information about selected calls, usually for cost allocation purposes.

Calling Party Restriction (CPR)
A setting within each Class of Restriction (COR) which allows or denies certain types of calls. For example, CORs with a CPR of "none" have no restriction, while CORs with a CPR of "outward" are not able to make any external calls.

Class of Restriction (COR)
Up to 96 (0 - 95) individual configurations of restrictions and permissions that control call origination and termination capabilities.

Class of Service (COS)
Assignments that determine certain calling options and features available to the telephone.

Control Circuit Packs
The circuit packs, or 'cards', not associated with stations or trunks, i.e. CPU, memory, software, and storage devices.

Coverage Answer Group
A group of up to 8 stations which act as an answer point for selected incoming calls. All phones in a Coverage Answer Group will ring simultaneously.

Coverage Path
A Coverage Path describes both the conditions under which incoming calls may be redirected and where they will be redirected.

Coverage Point
One of up to 6 answer points within a Coverage Path.

Direct Access
The ability of a station or trunk user to dial a Trunk Access Code (TAC) and receive dial-tone directly from a trunk, thus bypassing any restrictions of ARS.

Direct Inward System Access (DISA)
A general telecommunications-industry term for the Remote Access feature. See Remote Access.

DND/SAC
Do Not Disturb/Send All Calls - A feature allowing a user to temporarily deny their station the ability to receive incoming calls.

DS1
Refers to a digital signal trunking facility, e.g., T1.

Extension
A dialable number assigned to a station, data module, Hunt Group, Terminating Extension Group, Vector, etc.

External Number
When used in this audit, an 'external number' refers to a sequence of at least seven digits beginning with an AAR, ARS, or Trunk Group Access Code. These calls will potentially hit the public network and incur toll expenses.

Facility Restriction Level (FRL)
An FRL is assigned to each Class of Restriction (COR) and is used to allow or deny access to specific Trunk Groups. An FRL of 0 is the most restrictive, while 7 is the least restrictive and can commonly access more facilities.

Facility Test Call
A feature which allows a technician to place calls directly to specific trunks or phones for testing and problem diagnosis, bypassing the normal permission restrictions.

Feature Access Code
A one to four digit code dialed by a user to activate a particular feature. For example, an administrator could define '*12' be used to activate the Call Park feature.

Hunt Group
Allows a call to a busy extension to be redirected to an idle extension within the group.

INADS Port
Initialization and Administration System Port - A port on the PBX which provides remote administrative access to PBX programming.

Intercom Group
A grouping of stations that have the ability to call each other by using a 1- or 2-digit code.

LWC Reception
A setting within station programming which tells the PBX where Leave Word Calling information will be stored.

NETCON Port
A NETwork CONtrol data module which provides administrative access to the Avaya PBX.

Operations Support System (OSS)
An alarm monitoring and notification system in the Avaya PBX that can inform personnel of unusual system events.

PBX
Private Branch eXchange - A private telephone system which provides connectivity and switching functionality for an organization.

Personal Station Access (PSA)
A feature which allows a user to associate their telephone programming with another station of the same type. This allows the user to move their programming from one phone to another. Similar to the TTI feature used by technicians.

Pickup Group
A group of stations that are able to answer calls to any of the stations within the same group.

Port
The physical location of terminal equipment using the addressing scheme of Cabinet, Carrier, Slot, Port.

Port Address
An alphanumeric value corresponding to a specific card and port within the PBX. Every trunk, station and Voice Mail port has a specific and unique Port Address.

Port Circuit Packs
The circuit packs, or 'cards', associated with stations and trunks, e.g. Digital Line Cards, Analog Trunk Cards, DS1 Interfaces, and Audix Voice Mail.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.