

Designing a Virtual Access Control Configuration Protocol for Implementation over ISDN and Shared-Media Networks

By: Chooi-Tian (Alex) Lee and J.W. Harris.
UNI-Net, Inc.
438 Colony Woods Drive
St. Louis, Missouri 63122.
Tel: (314)-821-1198
E-mail: jwharris@mo.net

Abstract

Digital technology enables unprecedented ability and ease in manipulating information. However, information manipulated with malicious intent is detrimental to individual privacy and discourages consumers and corporations from participating in electronic commerce. The encroachment of digital technology into our lifestyle and corporate environment has given rise to the need for individuals to safeguard personal information, and for organizations to protect trade-secret information either stored in computers or transmitted over LANs and WANs. A secure network and communication environment requires the services of encryption mechanisms, user password authentication, and network and user-interface based access control schemes that prevent unauthorized access to application programs and operating systems. While various encryption and authentication security mechanisms have garnered a lot of development effort, access control schemes using a virtual dedicated-media network system have not been fully developed. A dedicated-media network enables the authorization of access based on non-repudiate authenticity of the source. This capability presently cannot be implemented in shared-media networks. The objective of this paper is to introduce a Virtual Access Control Configuration Protocol (VACCP) which provides a dynamic security access authorization mechanism. VACCP performs token-based access security control to an application's user-interface resources. The VACCP security program is designed to control remote access for both the shared-media and dedicated-media mode of communication. VACCP security measures are implemented as a network Session-layer protocol which governs access capability and assigns access authorization to each application program on a per-user-basis.

1 Introduction

Digital technology has given us unprecedented ability and ease in manipulating information. However, malicious manipulation of information has had detrimental effects on individual privacy and the willingness of consumers and corporations to participate in electronic commerce. Various methods to secure information and control access have been utilized. Encryption of information and the use of digital signatures are utilized to safeguard information during transmission. Private-key password authentication methods, such as Kerberos, are used to authenticate the user identity and right of access to a computer system. However, an effective secure network environment is best achieved by developing the capability to dynamically allocate and control access to the application user-interface resources based on application usages, mode of communication, and user privilege on a per-user-basis. VACCP is designed to perform in this manner.

2 Current Situation

2.1 Insecure Network Architecture

Presently, the shared-media Internet, built upon TCP/IP, is inherently insecure for electronic commerce. Since information is routed from computer to computer, it is open and available for illegal viewing, seizure, hijacking for manipulation, and impersonation. *The crux of the security problem in the shared-media Internet is the use of broadcast routing and routing address identification schemes which are vulnerable to and facilitate illegal seizure, and impersonation.* As an example, IP uses non-selective multicasting of information among interconnected intermediary IPOP computers resulting in the exposure of the transmission information to illegal seizure. Also, the packet's source and

destination addresses are encoded within the IP MAC header which allows hackers to clone the IP's MAC address resulting in anonymous intrusion to a network's resources.

2.2 Firewall Systems Does Not Prevent Internal Threat

Firewall software systems are used to determine and grant local or remote access to a protected or trusted network by using password schemes to authenticate the identity of the user and the use of packet-filtering to control access. Once the firewall system has granted a user access to the trusted network, all application programs and computer resources connected to the trusted network are available to any authorized user. Firewall systems presently do not provide adequate protection against malicious intents from authorized internal network users. Furthermore, in order for a trusted network or Intranet to interface with the public Internet, a security proxy network server system is required as an intermediary communication between the trusted network system and the external network systems.

2.3 Inability of Security Software to Govern Application Read, Write, and Execute Functions

Firewall software and hybrid firewall software are utilized to create secure networks within a shared-media network environment. However, present firewall and hybrid firewall software are presently not designed to operate within a connection-based communication environment. Also, application and network level gateway security schemes do not have the ability to govern and control access to the application control functions or user-interface resources at the network level. This means that when a user has been authorized access to an application, the user has full access to all the application's user-interface read, write, and execute control functions. When such full access to an application's control functions is granted, a security hole is created through which the application can be used as a means to breach the trusted network security.

3 Implementation of Network Security

A lot of development efforts have been directed toward encryption and authentication security mechanisms. *However, the security protocol proposed herein is based on the belief that the most effective security protocol can best be achieved with a method that creates non-repudiate authentication of the source of a communication and has the ability to specify remote access control privileges to an application's user interface resources.* The paper advocates the use of connection-based communication links having reliable

connection-based access authentication. The paper proposes the use of security access authorization mechanisms based on mapping security tokens to application user-interface resources. This paper covers the creation of a unique network-level and application-level security scheme which sets up access capabilities to the application user-interface control functions. Access approval is based on user security access token authorization levels and the mode of communication. This unique security scheme is implemented at the perimeter of the computing resources and within the network protocol. It is established during the connection initialization handshake. It can be implemented in both the shared-media and dedicated-media network environment. Existing connection-based access authentication schemes can be use with the proposed security program to verify access to secure applications in a dedicated-media network. Existing user password authentication and information encryption security mechanisms are also incorporated. The following explains existing security mechanisms and software and the proposed security mechanism and software.

3.1 Network Security Mechanisms

There are several methods to protect a network system from unauthorized access. Network security mechanisms are many and can be categorized under the following methods:

- Packet filtering
- Connection-based data-link gateway
- Network level gateway
- Application gateway
- User-interface resources gateway
- Authentication
- Encryption

Packet filtering. A packet filtering routing server examines the MAC address of each incoming packet. The firewall server accepts messages from certain servers or nodes and drops others after authenticating with a database containing pre-approved MAC address information.

Connection-based data-link gateway. A connection-based data-link gateway mechanism is implemented within switched-based network switches and interfaces. This gateway handles information access to the switch's ingress and egress ports. Prior to information transfer, the communicating end-systems establish a virtual circuit connection. During connection establishment, the address translation tables of all network switches along the virtual circuit connection path are programmed to associate a connection identifier with the switch ingress and another connection identifier with the switch egress. The ingress and egress connection identifiers, such as ATM VCI/VPI, are not destination routing addresses but instead are information

handling identifiers. The network switch authenticates all incoming information connection identifiers with the switch address translation table to determine whether or not the information has access to the appropriate ingress ports. If an incoming connection identifier is determined not to have access to any of the switch's ingress ports, the information is dumped. When the switch writes the information to an egress port, the switch attaches the appropriate new connection identifier to the information so that it will be accepted by the next connecting switch.

Network level gateway. This network level gateway connects a remote port or end-point to a local destination port or end-point. For example, with TCP/IP, an access control mechanism on the gateway determines whether the remote user connected to the TCP/IP port is coming from a source authorized to use the destination TCP/IP port. If the user is authorized, the message is passed on without review.

Application gateway. The application gateway restricts incoming traffic to a specific application, such as e-mail or Web applications. Likewise, outgoing traffic can be restricted to originate from specific applications.

User-interface resources gateway. This gateway represents the proposed security mechanism that restricts incoming traffic to specific user-interface resources. The user-interface resources include send, receive, read, write, edit, delete, and execute functions to the application. An application user-interface resources functionality level is associated with a user-interface security token value. An access control mechanism on the gateway uses the security token to determine whether or not the user has such authorization to the application control and data user-interface resources. Likewise, outgoing traffic can be restricted to specific user control and data interface control functions.

User Authentication. User authentication software normally uses the Challenge Handshake Authentication Protocol (CHAP) mechanism incorporating either private-key or public-key using a synchronous or asynchronous password token to authenticate the user identity. When the access mechanism clears the user's key, it unlocks access to the host computer.

Information Encryption. Information encryption is used to defeat eavesdropping on information during transmission in both connection-based and connectionless-based communication. In connectionless-based communication, such as the Internet, information is broadcast among intermediary computers allowing hackers the opportunity to use code analyzing software to sense and capture information. Encryption of information allows private communication over broadcast communication networks. This transmission method for connectionless-based communication is also known as point-to-point tunneling protocol.

3.2 Firewall and Access-Control Software

The two modes of communication on a network protocol basis are termed dedicated-media and shared-media communication. In dedicated-media communication, a connection path or circuit has to be established between two communicating end-systems before information is transferred. In short, a dedicated-media network implements a connected-based or direct line of communication. With a shared-media network, there is no need to establish connections between communicating end-systems. In a shared-media network, information is broadcast to all end-systems connected to the network router. The broadcast of information over a shared-media network is also known as connectionless-based communication or a party line type of communication.

The security software used to control local and remote network communication within the two different modes of communication are firewall software and access-control software. Both are designed to prevent unauthorized access. The firewall software design is primarily based on the packet filtering method and is used in shared-media networks. Firewall software provides single-tiered access control, that is, all authorized users have equal access to all software on the trusted host computer. Access-control software was designed for connection-based network systems. Access-control software is best utilized in a true end-to-end connection-oriented communication environment and allows flexible, multi-tiered access control. Figure 1 depicts the differences between firewall (single-tiered access) and access-control (multi-tiered access) software.

Enhancing firewall and security access-control software is accomplished by incorporating other security gateway programs. Present security gateways provide varying degrees of network and application access control services. Our proposed security software provides network, application, and *user-interface resources* access control services. Security gateways usually use token mapping schemes to associate with security attributes. Mapping tokens with security attributes allows flexibility in implementing security measures as well as ease of implementation in a cross-platform network environment. Implementing token-based security gateway between end-systems involves three steps:

1. An initialization handshake between the two hosts in order to agree upon a set of security attributes, then security tokens are generated. The generation of tokens may include the use of a token server for creating token values for each system or a group of systems.
2. Attributes are mapped to tokens or recovered from tokens through an access control handshake between either the connecting host computer and the token server.

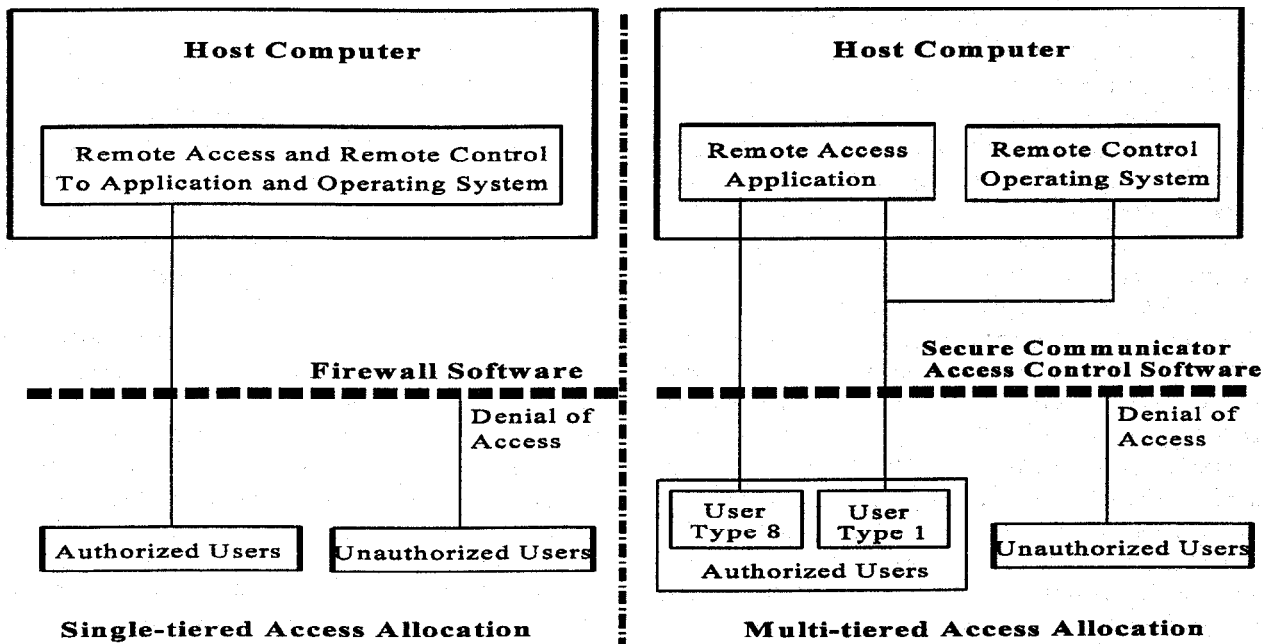


Figure 1: Differences between Firewall and Access-Control Software.

3. The token values incorporated into each datagram are used by a security enhanced computer to filter access.

CIPSO and SATMP are two of the most popular standardized security protocol for providing network security. This following discussion briefly covers the two network security protocols and introduces the new network security protocol, Virtual Access Control Configuration Protocol (VACCP).

3.2.1 CIPSO is Designed for Network level Gateway

Common IP Security Option (CIPSO) is one method of providing network security over current shared-media IP networks[1]. This CIPSO scheme is used to perform security decisions involving routing of IP datagrams at the IP network layer. It is a *network level gateway* which allows IP to govern connections of an external TCP/IP port to an internal destination TCP/IP port. The CIPSO security data is comprised of the Mandatory Access Control Sensitivity Security Policy (MACSSP) label. The MACSSP label is made up of a Sensitivity Hierarchical Level (SHL) and a set of Sensitivity Categories (SC). An IP datagram is allowed to be routed through a network interface device after the embedded CIPSO security data meets or exceeds the MACSSP label conditions. This means that users of network interfaces having higher MACSSP authorization can still view, seize, or

manipulate the datagram within shared-media networks.

3.2.2 SATMP for Governing Access to Applications

Security Attributes Token Mapping Protocol (SATMP) is another method for providing *network and application gateway* security measures over current shared-media IP networks[2]. SATMP uses token-based attribute identifiers to associate with applications, thus, security attributes can be extended to the application. SATMP restricts incoming information traffic to a specified application on the trusted computer. With SATMP, after the initialization handshake, each host begins by *assuming* that all communication uses connection-oriented schemes. *In reality, SATMP is designed to operate with IP which uses a broadcast communication scheme. Thus, SATMP is truly implemented over a point-to-broadcast-to-point communication link. It is through this intermediary broadcast communication link that SATMP is vulnerable to security breaches.*

3.2.3 Virtual Access Control Configuration Protocol

This proposed security scheme incorporates a unique security access-control mechanism termed Virtual Access Control Configuration Protocol (VACCP). VACCP is designed for a cross-platform environment. VACCP uses

token schemes to achieve interoperability among differing computer systems and to associate with differing security attribute requirements. VACCP applies *classification methods* to security access control attributes.

VACCP permits the negotiation and dynamic assignment of access resources to each virtual endpoint communication. The access resources for each endpoint is defined and established during connection establishment or initialization. Each endpoint is associated with a remote application control or data channel or port resident on either a shared-media or dedicated-media network. Since each endpoint is associated with an application program data or control channel, user-interface access privileges can be assigned to each application data and control channel. This concept allows a means to associate individual users with a specific application since each user is associated with a set of unique endpoint identifiers. The concept also allows a means to authorize differing access privileges which can be tailored to the type of dedicated-media or shared-media mode of communication.

Presently, all computing network protocol communications use a broadcast mode of communication at the network data-link level. Consequently, a broadcast mode of communication in a shared-media network creates network security vulnerability. Therefore, to assure a secure communication, communication links among remote application programs, over a network, should preferably be on an end-to-end connection-oriented basis. The benefit of having connection-based switching is that a secure, private, direct line of communication to application control functions is implemented over a dedicated-media network. The VACCP security program is designed to allow high access privileges for a dedicated-media mode of communication. When an application uses a shared-media network, constraint of access to an application's user-interface is imposed by allocating low VACCP access privileges. *This is done in anticipation that the communication links to application control and data user-interface resources can be compromised when non connection-based information routing schemes are used over a network.*

The approved VACCP access authorization parameters are encoded within the appropriate FAL information element field[3]. Access allocation is implemented in an efficient and scalable way by using a query mechanism to the VACCP program. The approved access allocation is linked to the FAL protocol code libraries during connection setup.

The VACCP security attributes access token is comprised of two sub-classes: the Application-Access Privilege (AAP) class and the User-Control Privilege (UCP) class. The AAP class defines the sensitivity level of access privilege to an application. The AAP class is used to associate public, privileged group, or private access authorization levels. The User-Control Privilege class defines the type of

access privilege to the application daemon commands or control user-interfaces. The User-Control Privilege identifiers are associated with the read, write, and execute capabilities of the application user-interface control functions. The type of user-interface access privileges assigned to a user are dependent on the user authorization levels and on the mode of network communication being used. By using different combinations of Application-Access Privilege and User-Control Privilege security attribute identifiers, a multi-tiered access authorization scheme can be configured to each application for each individual users.

A User-Control Privilege checking mechanism can be implemented, depending on the level of security requirements, to scan and authenticate any incoming command message accessing the application. The User-Control Privilege checking scheme is more effectively implemented when application control messages are encapsulated within a separate user control frame[4]. When a communication session request from a remote user is submitted during a connection setup, the VACCP program locates the remote user's session access authorization classification based on the requested application, the mode of communication, and the user and source identities. The VACCP program then assigns the appropriate AAP and UCP token values for that remote user. In summary, security access allocation is dependent upon the mode of communication. VACCP takes into account whether a shared-media or dedicated-media mode of communication is used when allocating access privileges.

3.3 VACCP-based Secure Communicator Program

There is a need to manage the types of access privileges for network-to-application communication links. The VACCP security software program consists of an object-oriented database containing classes of security access objects. VACCP security software can be implemented within a network routing firewall server in a shared-media network environment. VACCP security software can also be implemented as a remote access-control security software program on a host computer which uses a connection-based network system. The VACCP security software program, termed the Secure Communicator, is designed to manage network-to-application communication access privileges. The Secure Communicator uses VACCP-based access-control technology to control and govern access to the application and to the application control functions by blocking unauthorized access. The Secure Communicator, using VACCP API, is designed with a sophisticated authorization mechanism having discrete and hierarchical access schemes. The proposed Secure Communicator functions as an access control token server. It is designed with an application programming interface for programming FAL's Session access protocol

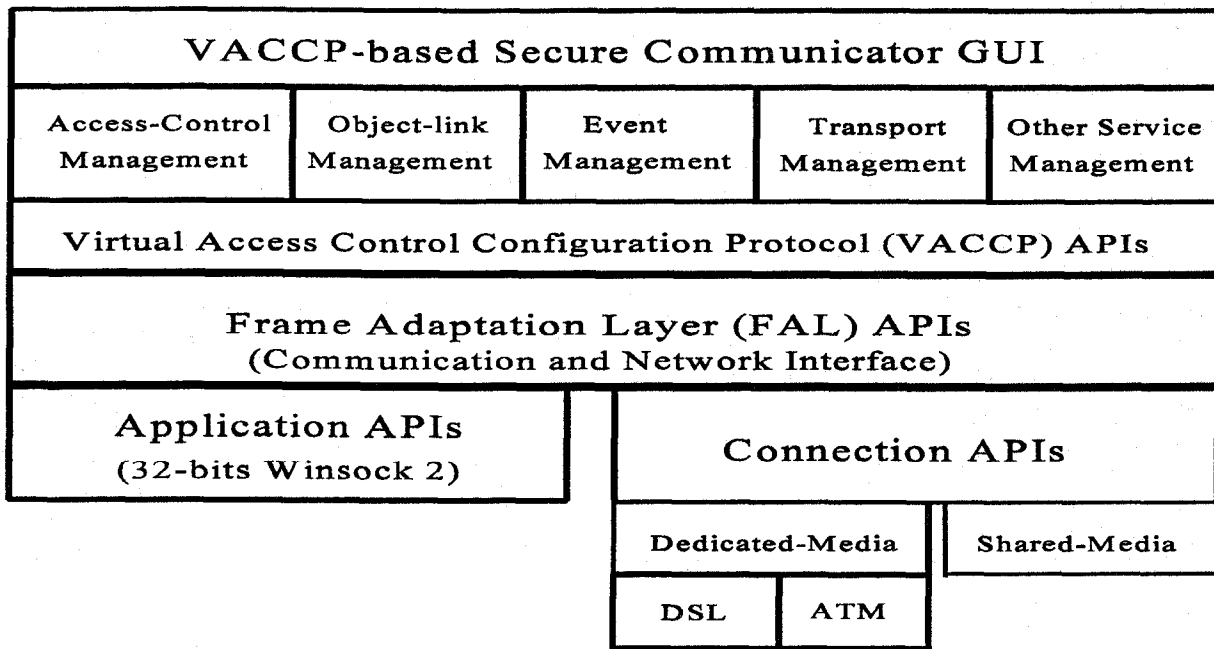


Figure 2: Secure Communicator API Links Architecture

code library module. Information packets, containing FAL protocol information elements and embedded VACCP security tokens, are layered on top of the ATM adaptation layer frames.[3][4]

The Secure Communicator also includes features having the ability to trace, monitor, and control the type of access for on-line commercial services. Consequently, the audit schemes, linked by handlers to the Secure Communicator, allow for tracing and identification of the source endpoint address of any unauthorized intrusion attempts to VACCP-enabled trusted networks. Existing connection-based call tracing, Caller ID, and call-back mechanisms can be implemented within the Secure Communicator. Since attempts at unauthorized access can be quickly and timely traced to the source device used, the threat of detection traceable to the source is a major deterrent in the prevention of fraud, malicious intents, and other criminal offenses.

As illustrated in Figure 2, the Secure Communicator forms the core security interface for anchoring access-control object handlers and forms interaction links between FAL protocol processing modules and application user interfaces. Using the Secure Communicator, end-users or network administrators can assign access rights to applications on a public, trusted group, private, or confidential basis. Service providers and end-users can also tailor and grant individuals or groups differing rights to read, write, or execute user-interface

functions for an application program resident on the same server or host computer. This is a prerequisite for secure commercial applications.

3.4 Use of Secure Virtual Dedicated-media Networks

The abilities to encrypt information for transmission, to authenticate the user identity, and to govern and authorize access to an application user-interface and device operating system based on the mode of communication, are required in order to provide a secure network environment for digital communication and computing. This paper advocates the use of ATM networks to create a more secure networking environment for electronic commerce and private communication. A *virtual dedicated-media Internet*, built around ATM and FAL protocols, would provide a more secure end-to-end connection-oriented information transmission.[5] Virtual dedicated-media Internet provides the opportunity to use the unforgeable dedicated-media connection scheme as an authentication parameter to design unique individual access authorization schemes. Virtual dedicated-media network routes information through a relay of switches from the caller end-system directly to the called end-system without flowing into any intermediary computers. *This direct line of communication eliminates an inherent*

network vulnerability associated with shared-media networks in that there are no intermediary computers that could be used as a tool for potential security breaches.

The ability to impersonate an authorized user is eliminated in a virtual dedicated-media network. A virtual dedicated-media network does not have the destination routing addresses encoded within the ATM cells. ATM cells use the ATM Header Layer VCI/VPI index. As an ATM cell is routed through an ATM switch, the ATM switch address translation table is used to determine whether an incoming ATM cell from an ATM ingress port should have access to the ATM switch. The ATM switch address translation table also encodes a new VPI/VCI index for a departing ATM cell so that it will be accepted by the next connecting network switch. In short, the destination routing path is established and encoded within an ATM switch address translation table during call connection establishment. This address registry table routing mechanism provides a strong defense against impersonation as a direct communication link must be established before any information is transferred through the communication link.

One might argue that dedicated-media networks can be wire-tapped. Since no scheme can be adequately secure without suitable encryption schemes for information transmission, the VACCP architecture includes an encryption mechanism as a linkable handler to be used when needed. A channel hopping algorithm mechanism can also be incorporated as a VACCP linkable handler for enabling the transmission of information among multiple SVCs in random order and intervals. Implementing channel hopping among the SVCs and using encryption of information adequately prevents the use of wire-tapping schemes for eavesdropping.

3.5 Allocation of Application Access based upon Usages

The VACCP-based security program determines the pre-approved user access attributes authorization after receiving a request for access authorization from the FAL protocol during a connection setup, and then assigns the access resource parameters for that connection. For high security applications, the approved access token is established only after both user identity and caller source authentication have been performed through challenge-response password authentication and Caller ID or call tracing checks. The security access-control program can be implemented on a host client or server computer.

The assignment of the VACCP communication session access authorization parameters is based on the usage of the application, the pre-approved caller access authorization, and the mode of communication.[4] For example, a web browser requires the ability to communicate with other web servers

over the shared-media Internet, and the web browser control functions may be openly available for use by the public. On the other hand, a financial transaction program requires the ability to have a restricted public user access to a financial transaction application server through virtual dedicated-media network communication. The financial transaction program may require that application daemon control capability for public users be limited to write only functions of the application data entry user interface. Thus, an access-control security attribute program should provide the ability to program application daemon control access authorization through use of application user-interface security attributes. The above described application usage situations and access privileges can be handled by VACCP security program. The VACCP security program is able to allocate the appropriate and differing access privileges for the Web and financial transaction programs even when they are resident on the same host computer.

3.6 Allocation of VACCP Security Attribute Identifier

VACCP architecture is designed to exploit the FAL protocol and packet-switching demultiplexing mechanisms. The VACCP server maintains an access attributes table or database. The table's access attributes, comprised of application ID, mode of communication, user ID, and security-attributes class identifiers and corresponding token values, are used to associate an application with the type of network connection and user privilege with application user-interface resources. During call connection establishment, FAL API queries the VACCP server for the required access tokens to the application by forwarding the application ID, network connection type, connection ID, and user ID. The application ID, network connection type, connection ID, and user ID provide a level of indirection through the access attribute table to obtain the appropriate Application Access Privilege and User-Control Privilege identifiers. The VACCP API then programs the resultant VACCP access authorization tokens, Application-Access Privilege and User-Control Privilege information elements, within the appropriate FAL protocol code library.

The Application-Access Privilege information element determines the application's privileges which could be designated as public, restricted group, private, or determines if access is denied. The User-Control Privilege information element determines the types of user-interface read, write, and execute resources that are to be allocated for the application command functions. On receiving the VACCP access authorization information elements, FAL can either terminate the connection or encode the access token values into the registry as an access session ID, depending on whether the

Table 1: Possible Security Measures and Policy Implementations

	Web Browser Server Application			Transaction-Application Program		
AAP Identifier	23			18		
Type of User Groups AAP Sensitive-Level Token Value	Public 10	Trusted 8	Private 1	Public 10	Trusted 7	Private 1
Types of network supported	SM/DM	SM/DM	DM	DM	DM	DM
Required Security Measures:						
Connection Authentication	No/No	Yes/Yes	Yes	Yes	Yes	Yes
Caller ID enabled	NA/No	NA/Yes	Yes	Yes	Yes	Yes
Call Trace enabled	NA/No	NA/No	Yes	No	No	Yes
Call Back enabled	NA/No	NA/No	Yes	No	No	Yes
Call Forward disabled	NA/No	NA/No	Yes	Yes	Yes	Yes
User Authentication	No/No	Yes/Yes	Yes	Yes	Yes	Yes
User Name	NA/No	Yes/Yes	Yes	No	Yes	Yes
Encrypted Password	NA/No	Yes/Yes	Yes	No	Yes	Yes
Encryption Key	NA/No	CHAP token	CHAP token	No	CHAP token	CHAP token
Message Encryption	No/No	Yes	Yes	No	Yes	Yes
Encryption type	NA/NA	Public-key	Public-key	NA	Public-key	Public-key
Algorithm Type	NA/NA	DES	DES	NA	DES	DES
Scan application executable frames	No/No	Yes/Yes*	No	No	Yes*	No
Channel Hopping enabled	NA/No	NA/No	Yes	No	Yes	Yes
Intrusion Audit Logging	No/No	Yes/Yes	Yes	No	Yes	Yes
IP Address	No/NA	Yes/NA	NA	NA	NA	NA
Non-repudiation Address	NA/No	NA/Yes	Yes	No	Yes	Yes
Time-stamping	No/No	Yes/Yes	Yes	No	Yes	Yes
Application Remote Access						
Capabilities: UCP Token:						
Open 16	Yes	Yes	Yes	Yes	Yes	Yes
Send 15	Yes	Yes	Yes	Yes	Yes	Yes
Receive 14	Yes	Yes	Yes	Yes	Yes	Yes
Input Save (Write to disk) 13	Yes	Yes	Yes	Yes	Yes	Yes
Read from disk 12	Yes	Yes	Yes	No	Yes	Yes
Output Save (Write to disk) 11	No	No	Yes	No	No	Yes
Execute 10	No	No	Yes	No	No	Yes
Computer Remote Control						
Capabilities: UCP Token:						
Read 7	No	No	Yes	No	Yes	Yes
Write 6	No	No	Yes	No	No	Yes
Delete 5	No	No	Yes	No	No	Yes
Edit 4	No	No	Yes	No	No	Yes
Load 3	No	No	Yes	No	No	Yes
Execute 2	No	No	No	No	No	Yes
Remote Log in 1	No	No	No	No	No	No

Definitions: NA - not applicable

SM - Shared-Media

DM - Dedicated Media

AAP - Application-Access Privilege

UCP - User-Control Privilege

* When application commands or executables information are separately encapsulated from application data information.

VACCP attribute identifiers indicate denial or approval of access. The approved access token values are also transmitted to the caller for programming at the caller end-system. The VACCP access token values are linked to the FAL endpoint_identifier-to-application_channel address and used to filter access during packet demultiplexing at the host computer.

4 Benefits

The proposed VACCP scheme makes it possible to dynamically allocate differing access security attributes for each user to each application. The primary goal of VACCP is to provide a communication means for safeguarding privacy and the security of proprietary information. VACCP is also designed to handle future real-time interactive multimedia application security requirements. It allows the access session of application command to be determined within the network protocol. Table 1 illustrates the unique operating features that the VACCP scheme has over existing shared-media firewall systems.

There are several factors that favor access-control protocol implementations that are dynamically linkable to network protocol. The most obvious is the ease of re-configuration and maintenance of application access authorization attributes. Other factors are:

1. VACCP mechanism allows multi-tiered access control to be implemented at both the network level and the application user-interface level.
2. VACCP mechanism is able to recognize whether the application is connected over a shared-media or a dedicated-media network and assigns the appropriate access security attributes based on the mode of network communication being used.
3. With VACCP, user-interface access scanning and filtering can be done at the network protocol-level.
4. VACCP security attributes mechanism is designed to operate within connection-oriented networks with connection-based communication links and connectionless routing network systems.
5. VACCP is design to utilize existing connection-oriented network service programs such as Caller ID and call tracing.
6. VACCP security token information element incorporated into FAL network protocol enables network protocol to be aware of the end-system application security requirements.
7. VACCP security mapping token system enables interoperability in a cross-platforms of network and computing environments.

5 Conclusion

A key feature of using VACCP security access-control architecture with FAL protocol is the ability of a server or a host computer to support secure communication over both dedicated-media and shared-media networks. This benefit represents a savings in cost in setting up secure interactive multimedia services since redundant proxy servers required for maintaining security can be eliminated. The trusted network is easier to maintain because VACCP uses automated and programmable outside-the-kernel security protocol libraries that can be easily upgraded. Furthermore, the ability to directly control access and traffic flow to any application user interfaces creates flexibility in the way each application communicates securely with other applications. This is not possible under present shared-media firewall systems.

The transfer of user interface access authorization checks from the application-level to the network protocol-level results in access filtering taking place at the perimeter of the application. Implementing the access-control session for application user-interface functions at the network protocol level enables the termination of unauthorized access at the perimeter of the computer resources. The use of network- and application-independent security attribute token values to determine access capabilities to specific application user-interface functions allows interoperability over various application, device operating systems, and network environments. The ability to restrict access to the application user-interface control functions and to quickly trace and report illegal access is a major deterrent to malicious access and intents. When used in a virtual dedicated-media network environment, VACCP enables connection-based checks and call trace on the sender or caller endpoints. VACCP can also be effectively implemented over existing shared-media network environments and provides the ability tailor a different user-interface access authorization for both the shared-media and dedicated-media mode of communication.

References

- [1] "Common IP Security Option", IETF CIPSO Working Group, March, 1993.
- [2] "Security Attributes Token Mapping Protocol", SECUREWARE, Inc., Aug 1994.
- [3] "A Versatile Frame Adaptation Layer (FAL) Architecture for ATM User Plane", Chooi-Tian Lee and J.W. Harris, UNI-Net, Inc., April 1996.
- [4] "Principle and Technique for Encapsulation of User Control and Data Information in Separate Frames", Chooi-Tian Lee and J.W. Harris, IEEE 21st Conference on Local Computer Networks, Oct 1996.

- [5] "Proposal for Developing a Secure Electronic Commerce Environment Using VACCP and Virtual Dedicated-Media Internet", Chooi-Tian Lee and J.W. Harris, UNI-Net, Inc., April 1996.