FIPS 140-2 Security Policy

3Com 10/100 Secure NIC (3CR990B-97) &
3Com 100 Secure Fiber NIC (3CR990B-FX-97)

3Com Corporation
5500 Great America Parkway
Santa Clara, CA 95052
USA

June 18, 2004

Revision Version 1.03

1. Introduction

The following describes the security policy for 3Com Corporation's 3Com 10/100 Secure NIC (3CR990B-97) & 3Com 100 Secure Fiber NIC (3CR990B-FX-97). The hardware version number for 3CR990B-97 is 03-0229-100 while that for 3CR990B-FX-97 is 03-0347-000. The 3CR990B family of NICs provides FIPS 140-2 validated IPSec (DES/3DES/SHA-1) offloading functionality. The firmware version of the sleep image running on the card is 03.001.007. The runtime and diagnostic images have firmware version number 03.001.008. The module is referred to as the 3CR990B throughout this document.

The 3CR990B is a PCI 2.2 based Ethernet Network Interface Card. It has an embedded ASIC that consists of among others ARM9 processor and an IPSec offload engine. The PCI interface allows the NIC to communicate with the host computer. The associated device driver and the firmware for 3CR990B allow the Operating System to offload IPSec functionality to the NIC adapter. Additionally, the flash firmware present on the NIC performs image authentication for all firmware modules downloaded to the NIC by the host system. Overall 3CR990B meets FIPS 140-2 compliance of security Level 1. The 3Com NIC is considered a multi-chip embedded module for FIPS 140-2 purposes.

1.1. Purpose

This document covers the secure operation of 3CR990B, including the initialization and the responsibilities for operating the product in a secure, FIPS-compliant manner.

1.2. Glossary

Term/Acronym	Description
NIC	Network Interface Card
OS	Operating System
PC	Personal Computer
MMC	Microsoft Management Console
SA	Security Association
CO	Crypto Officer
EDC	Error Detection Code

2. Roles, Services, and Authentication

2.1. Roles

The module supports the following two roles:

User Role

The User role is assumed by any entity requesting the services of the card, both cryptographic and non-cryptographic. The User can send and receive both encrypted and unencrypted data using the NIC. The User can also configure the NIC settings using the NIC Doctor diagnostic utility and gather and view NIC statistics. In the User Role, i.e. when a non-administrative user is logged on the OS, the user cannot enable or disable 3CR990B. They also cannot alter the IPSec policy setup on the PC. They can only transmit and receive packets as per the IPSec policy active on the PC. Only one User role is supported.

Crypto-officer Role

The Crypto-Officer (CO) is responsible for installing the NIC and corresponding drivers and diagnostic software on the PC. Typically a user needs administrative privileges for the OS to be able to install a NIC. 3CR990B is first installed on the PC system using the conventional installation procedures as pertains to the underlying OS. The Crypto-officer Role (i.e. the Administrator in OS context) has privilege to install/uninstall, enable/disable and configure the NIC. The CO must also configure the Windows Operating System for IPSec and ensure that encryption and data-authentication offloads are done on the NIC. They can setup policies (i.e. IPSec offload, 3DES/DES, SHA-1/MD5) for the PC. Setting up the IPSec policies also requires Administrative privileges on the PC. Such policies are then enforced on any user that uses the PC. Only one Crypto Officer role is supported.

2.2. Services

At any given time 3C990B can execute only one firmware image. The following images provide services to the User and Crypto Officer.

1. Runtime image: This firmware image is the operational image of the module and is responsible for providing the IPSec offload function to the host OS. This image must be loaded on the card memory by the device driver

2. Diagnostic image: In addition to the services provided the runtime image the diagnostic image also provides additional diagnostic capabilities. This image must be loaded on the card memory by the device driver

3. Sleep image: This image is stored in the FLASH memory on the card and is automatically loaded when the module powers-up.

4. Reflash image: This image allows the flash memory to be upgraded to a new digitally signed flash image. The device driver must load this image on the card memory when the FLASH image needs to be updated.

The services provided by the respective images are defined below. Common Services are services that are provided by all images.

Service	Description	Role
COMMON SERVICES		
Transmit enable	Enable packet transmission onto Ethernet interface	User/Crypto-Officer
Transmit disable	Disable packet transmission onto Ethernet interface	User/Crypto-Officer
Receive enable	Enable packet reception from Ethernet interface	User/Crypto-Officer
Receive disable	Disable packet reception from Ethernet interface	User/Crypto-Officer
Read receive filter	Read current receive filters	User/Crypto-Officer
Set receive filter	Set receive filter to given value	User/Crypto-Officer
Read Statistics	Return the Statistics table to host	User/Crypto-Officer
Read flash page	Read the specified flash page	Crypto-Officer
Write flash page	Write to the "data only" flash pages	Crypto-Officer
Enable PHY loopback	Enables loopback of packets at the PHY interface	User/Crypto-Officer
Disable PHY loopback	Disables loopback of packets at the PHY interface	User/Crypto-Officer
Add multicast address	Adds a new multicast address to receive packets	User/Crypto-Officer
Set MAC address	Sets the station MAC address to that specified	User/Crypto-Officer
Read MAC address	Reads the current MAC address	User/Crypto-Officer
Read VLAN type	Reads the current VLAN type	User/Crypto-Officer
Write VLAN type	Sets the VLAN type to that specified	User/Crypto-Officer
Issue software reset	Performs software reinitialization	User/Crypto-Officer
Issue software halt	Stops the current firmware image from executing	User/Crypto-Officer
Read version information	Reads the current image's version information	User/Crypto-Officer
Set interrupt coalescing	Enables/Disables interrupt coalescing	User/Crypto-Officer
Read PCI config register	Reads the specified PCI Configuration register	User/Crypto-Officer
Write PCI config register	Sets the specified PCI Configuration register	User/Crypto-Officer

Get link status	Returns the link status (connected/disconnected)	User/Crypto-Officer

SLEEP SERVICE		
Add wakeup events	Allows host to add wakeup patterns to 3C990B	Crypto-officer
Enable sleep events	Allows host to perform events like Respond to Ping	Crypto-officer
Enable wakeup events	Allows host set wakeup events like Wake-On-Ping	Crypto-officer
Firmware Image Download	Allows download of firmware images to 3C990B	User/Crypto-Officer

RUNTIME SERVICE		
Add Security Association	Adds a new security association provided by host	User/Crypto-officer
Delete Security Association	Deletes an offloaded security association	User/Crypto-officer
Transmit IPSec packets	Encrypts and transmits IPSec packets	User/Crypto-officer
Receive IPSec packets	Decrypts and receives IPSec packets	User/Crypto-officer

DIAGNOSTIC SERVICE		
Test ARM2HOST registers	Tests the ARM to HOST registers	Crypto-officer
Test HOST2ARM registers	Tests the HOST to ARM registers	Crypto-officer
Test PCI DMA	Tests the PCI DMA interface	Crypto-officer
Test PCI interrupt	Tests the PCI interrupts	Crypto-officer
Test receive interrupt	Tests receive MAC interrupts	Crypto-officer
Test transmit interrupt	Tests transmit completion interrupts	Crypto-officer
Set encryption level	Allows host to set encryption levels like DES/TDES	Crypto-officer
Test oneshot timer	Tests the one shot timer on 3C990B	Crypto-officer

REFLASH SERVICE

Flash Image Update	Allows flash image to be updated	Crypto-officer
Zeroize HMAC SHA-1 Key	Sets the HMAC SHA-1 Secret Key to Zeros	Crypto-officer

2.3. Authentication Mechanisms and Strength

The module does not provide authentication for any role. A role can be assumed implicitly by requesting services which have been assigned to that role.

Firmware Authentication

The module does authenticate firmware uploads by using an Approved authentication technique in the form of HMAC-SHA1. 3CR990B requires the host to download a digitally signed firmware image from 3Com. The NIC authenticates the firmware module by re-computing and comparing the HMAC SHA-1 digest, using 3Com's HMAC-SHA1 Secret Key stored in FLASH. If the firmware module fails authentication, 3CR990B enters a failure mode and becomes non-functional. Crypto offloads and packet transmission or reception are blocked. To recover such 3CR990B NIC the PC has to be reset. Any new firmware that is uploaded on the card must be FIPS 140-2 validated.

3. Secure Operation and Security Rules

In order to operate 3CR990B and to utilize the IPSec offload function the Crypto Officer must know how to configure Microsoft Management Console (MMC) for Windows Operating System. Once the policies are setup to offload IPSec session, the OS will automatically initiate and setup IPSec session with a remote client and then offload the crypto functions for that session to the NIC.

3.1. Security Rules

The security rules enforced by 3CR990B include both the security rules that 3Com Corporation has imposed and the security rules that result from the security requirements of FIPS 140-2.

3Com Security Rules

The following are 3Com security rules:

1. 3CR990B shall store the HMAC SHA-1 Secret Key.
2. 3CR990B will not store any IPSec session keys in its non-volatile memory.
3. 3CR990B shall never output the Secret Key or the IPSec Session Key.

FIPS 140-2 Security Rules

The following are security rules that stem from the requirements of FIPS PUB 140-2. The module enforces these requirements when initialized into FIPS Level 1.

1. When initialized to operate in Level 1 mode, 3CR990B shall only use FIPS-approved cryptographic algorithms.
2. 3CR990B shall provide the Crypto Officer the capability to zeroize the HMAC SHA-1 secret key stored in the flash. It will also zeroize the IPSec session key when the OS deletes the Security Association (SA).
3. 3CR990B will only allow to load and run digitally signed firmware module from 3Com Corporation.
4. 3CR990B will also perform self-test and know answer tests of all crypto components during power-up. On any failure the unit will become non-functional.
5. 3CR990B will validate the on-board firmware using 16bit EDC checksum.
6. Flash firmware on 3CR990B shall be upgraded only with a digitally signed flash image from 3Com.
7. The Crypto-Officer shall not configure IPSec policies that use MD5, HMAC-MD5 for IPSec.
8. The module must be run on a Windows 2000 OS and the associated device driver provided by 3Com.
9. 3CR990B will only transmit encrypted IPSec traffic in an Approved mode of operation. The NIC should not be used to transmit plaintext data over the network in an Approved mode.
10. The module is always in an alternating bypass mode providing cryptographic and bypass services depending on the packet IP header.

3.2. Secure Operation Initialization Rules

3CR990B provides many different cryptographic algorithms to ensure compatibility with today's marketplace. Specifically, the 3CR990B provides the following algorithms:

Algorithm Type	Key Sizes/ Modes	FIPS-approved
Symmetric Algorithms		
TDES (Cert. #212)	168-bit, CBC & ECB	Yes
DES[1] (Cert. #234)	56-bit, CBC & ECB	Yes
Hashing Algorithms		
SHA-1 (Certs. #188 and #189)	Byte-oriented	Yes
MD5		No
Authentication Algorithms		
HMAC-SHA1 (Certs. #188 and #189, vendor affirmed)		Yes
HMAC-MD5		No

Because FIPS 140-2 prohibits the use of non-FIPS approved algorithms while operating in a FIPS compliant manner, the Crypto Officer should follow the following rules to initialize a new 3CR990B to invoke the Approved mode of operation.

1. Power-up the PC with 3CR990B.
2. After the OS loads, install the device driver for 3CR990B using the installation CD.
3. After the NIC is installed, setup the system IPSec policy using MMC. Refer to Microsoft System Administrator's Guide for more details on MMC. The Crypto Officer must create such IPSec policies on the Windows Operating System that only use FIPS Approved algorithms (SHA-1 for AH and DES/TDES, SHA1 for ESP). MD5 and HMAC-MD5 should not be used in an Approved mode. Furthermore, the IP Security rules and IP Filter actions must be configured to only allow IPSec traffic to flow on all network connections. The configuration must disallow communication with computers that do not support IPSec.
4. Once the IPSec policies are defined, all sessions initiated or received by the PC will be encrypted.
5. The OS will then offload the IPSec session and its SA's to 3CR990B.
6. Once IPSec sessions are offloaded to 3CR990B, it will encrypt/decrypt any IPSec traffic that matches the SA.

[1] DES must be used only on legacy systems. 3Com recommends use of TDES to protect sensitive data.

4. Definition of SRDIs Modes of Access

This section specifies 3CR990B's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by it.

4.1. Cryptographic Keys, CSPs, and SRDIs

While operating in a level 1 FIPS-compliant manner, the 3CR990B NIC contains the following security relevant data items:

Security Relevant Data Item	SRDI Description
HMAC SHA-1 Secret Key	A 512-bit HMAC SHA-1 secret key embedded within the 3CR990B's Flash memory. This key is used to verify the signature attached to a downloaded firmware image.
IPSec Session Keys	The OS offloads the IPSec session keys (DES/TDES keys for encryption and HMAC-SHA1 keys for data authentication) to 3CR990B and they are stored in the volatile RAM memory on 3CR990B. These keys are zeroized when the OS deletes the SA or when 3CR990B is powered off.

4.2. Access Control Policy

3CR990B allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SRDI while operating the NIC in a given role. These access control policies cannot be changed or modified by any role within the module. The permissions are categorized as a set of three separate permissions: read (R), write (W) and use (U). If no permission is listed, then an operator has no access to the SRDI. Only those services that provide any access to the SRDIs are listed below. All other services from the Services table in Section 3 above do not provide any access to the SRDIs of the module.

3CR990B SRDI/Role/Service Access Policy	Security Relevant Data Item	HMAC SHA-1 Secret Key	IPSec Session Keys
Role/Service			
User role			
Transmit IPSec packets (encrypt)			U
Receive IPSec packets (decrypt)			U
Add Security Association			W
Delete Security Association			W
Firmware Image Download		R/U	
Crypto-Officer Role			
Transmit IPSec packets (encrypt)			U
Receive IPSec packets (decrypt)			U
Add Security Association			W
Delete Security Association			W
Firmware Image Download		R/U	
Flash Image Update		R/U	
Zeroize HMAC SHA-1 Key		W	

5. Self-tests

The module provides the following power-up and conditional self-tests

5.1. Power-Up Tests

These are performed when the module boots up.

- DES CBC Known Answer Test for the hardware implementation
- 3DES CBC Known Answer Test for the hardware implementation
- HMAC-SHA1 Known Answer Test for the hardware implementation
- SHA1 Known Answer Test for the hardware implementation
- HMAC-SHA1 Known Answer Test for the firmware implementation
- A 16-bit Firmware Integrity Check on all firmware
- HMAC-SHA1 Known Answer Test for the firmware implementation in the flash upgrade utility.

5.2. Conditional Tests

The following load test is performed when a firmware image download is requested.

- Firmware Load test: The module performs an HMAC-SHA1 keyed hash verification of each image that is downloaded on the card. The module enters an error state in case of self-test failures and does not provide any functionality. It must be reset to recover from the error state.
- Bypass self-test: The module performs a bypass self-test on each packet which is sent out in plaintext. If the test fails, the packet is dropped.

6. Mitigation of Other Attacks

This section is not applicable as the module does not provide mitigation against any commonly known attacks.