The following paper was originally published in the
Proceedings of the USENIX Windows NT Workshop
Seattle, Washington, August 1997

Implementing Security and Mobility Functions in Kernel Drivers

Yoshiyuki Tsuda, Masahiro Ishiyama, Atsushi Fukumoto, and Atsushi Inoue
R&D Center, Toshiba Corporation
Ken-ichi Yokoyama
Fuchu Works, Toshiba Corporation

For more information about USENIX Association contact:

1. Phone: 510 528-8649
2. FAX: 510 548-5738
3. Email: office@usenix.org
4. WWW URL: http://www.usenix.org

Implementing Security and Mobility Functions in Kernel Drivers

Yoshiyuki Tsuda, Masahiro Ishiyama, Atsushi Fukumoto and Atsushi Inoue
R&D Center, Toshiba Corporation
Ken-ichi Yokoyama
Fuchu Works, Toshiba Corporation

Abstract

We are developing a secure, mobile network system, named "Network CryptoGate (NCG)", which provides a secure Virtual Private Network (VPN) environment for mobile users seamlessly, even if they move to an insecure network. NCG is designed upon IETF standards, that is IP security (IPSEC) and Mobile IP (MobileIP), in order to make the whole system interoperable with other implementations. Currently, we have developed an NCG client software on Windows NT [1]. At the poster/demonstration session, we will demonstrate how an NCG client works.

1. System Overview

There are two major components in the NCG network system: NCG servers and NCG clients, as illustrated in Figure 1.

As a VPN server, an NCG server performs encryption and authentication for all packets that leave the private network, while for all incoming packets it decrypts and checks the authentication. As a mobility agent, an NCG server intercepts those packets which bound for a moved NCG client, and transfers them to the NCG client's current location. We have already implemented NCG servers are on BSD and Solaris [2], and are currently porting them to Windows NT [1].

An NCG client is a client software on a mobile terminal. When a mobile terminal leaves the private network, an NCG client encrypts and authenticates all packets bound for the private network, and decrypts all packets received from that network and checks their authentication. Also, an NCG client performs Mobile IP functions as a mobile terminal. We have developed NCG clients on Windows NT, and are now porting them to Windows 95 [1].

[1] "Windows NT" and "Windows 95" are registered trademarks of *Microsoft Corporation*.

[2] "Solaris" is a registered trademark of *Sun Microsystems, Inc.*.

2. NCG client software architecture

A current NCG clients consists of an NDIS driver, a transport driver and application program, as illustrated in Figure 2. When a mobile terminal leaves the private network, all packets from/to the TCP/IP driver are processed by the MobileIP/IPSEC modules in the transport driver so as to preclude any impact on the TCP/IP driver and the upper software modules, as well as the card driver. Thus, we can provide a secure, seamless VPN environment for mobile users.

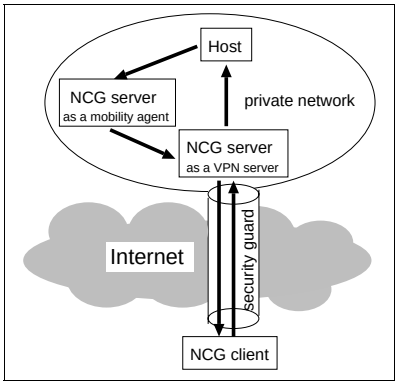

Figure 1. NCG system overview

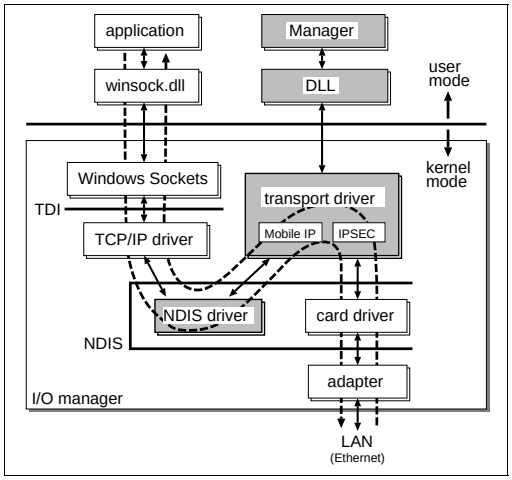

Figure 2. NCG client software architecture