IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No. 6,502,135	)		
	)		
Filed: February 15, 2000	)	Group Art Unit:	Central Reexamination Unit
	)		
Issued: December 31, 2002	)		
	)	Examiner:	
Inventors: Munger et al.	)		
	)	Confirmation No.:	
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY	)		

REQUEST FOR INTER PARTES REEXAMINATION UNDER 35 U.S.C. § 311

ATTN: Mail Stop Inter Partes Reexam
Central Reexamination Unit (CRU)
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir,

Presented herewith is a request for *inter partes* reexamination of United States Patent No. 6,502,135 (the '135 patent), entitled "Agile Network Protocol for Secure Communications with Assured System Availability." The inventors of the '135 patent are Edmund Colby Munger, Douglas Charles Schmidt, Robert Dunham Short, Victor Larson and Michael Williamson. The present assignee of the '135 patent is VirnetX Corporation, as recorded at Reel 018757, Frame 0326. A list of all exhibits submitted with this reexamination request is provided in the accompanying transmittal letter for this request for inter partes reexamination.

tunnels. *See* Beser at col. 1, l. 54 to col. 2, l. 18. Beser also points out the importance of assuring the secure and private nature of IP tunnels between the first and second network devices. *See, e.g.*, *Id.* at col. 2, ll. 36-40 ("It is therefore desirable to establish a tunneling association that hides the identity of the originating and terminating ends of the tunneling association from the other users of a public network. Hiding the identities may prevent a hacker from intercepting all media flow between the ends."); col. 12, ll. 13-19 ("In this manner, the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network. The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26).") Beser further explains other than situations where it would be impractical, VPNs and encryption of IP traffic in IP tunnels using the IPsec protocol should be used. *See id.* at col. 1, l. 54 to col. 2, l. 18.

Kent describes use of IPSec to establish VPNs including by IP tunneling. *See, e.g.*, Kent at 8 ("A tunnel mode SA is essentially an SA applied to an IP tunnel.") The IPSec protocol calls for encryption of all IP traffic being sent between nodes of the VPN network – the protocol is designed to automatically encrypt traffic being sent between nodes.

Kent also teaches that the encryption and tunneling mechanisms of IPSec work automatically. In particular, in the IPsec protocol, outbound and inbound IP packets are examined and afforded the specified protection based on the IP and transport layer header information (e.g., the outbound packet is analyzed and encrypted according to a specified method). This occurs automatically according to policies that have been established for the connection. *See generally id.* at 13 (describing handling of inbound and outbound IPsec traffic); *Id.* at 29-34 (describing the protocols for handling outbound and inbound IP packets).

A person of ordinary skill in the art would have relied on Kent to modify the design of Beser to incorporate IPsec to encrypt all traffic being sent in IP tunnels between a first and second network device in the IP tunneling procedures being described in Beser, rather than to encrypt only the traffic used to establish the IP tunnel. Accordingly, Beser in view of Kent would have rendered obvious claim 1 under 35 U.S.C. § 103.

2. Claim 2

Claim 2 depends from claim 1, and specifies that steps (2) and (3) of claim 1 are performed at a DNS server separate from the client computer.

Beser expressly describes processes and systems where the DNS server (the trusted third party network device) is separate from the client computer (the first network device that generates the request). In particular, Beser explains that the trusted-third-party network device can be a domain name server, and that this device is a distinct network device from the first network device. *See, e.g.*, Beser at Figures 1 and 4; at col. 2, ll. 50-56 ("The method includes receiving a request to initiate the tunneling association on a first network device. The first network device is associated with the originating end of the tunneling association, and the request includes a unique identifier for the terminating end of the tunneling association. A trusted-third-party network device is informed of the request on a public network."); and col. 11, ll. 33-35 ("In one exemplary preferred embodiment, the trusted-third-party network device is a

VIII. CONCLUSIONS

Based on the explanations provided herein, Requester believes that substantial new questions of patentability have been established for each of claims 1-18 of the '135 patent. Requester accordingly submits that an *inter partes* reexamination should be established, and claims 1-18 of the '135 patent should be rejected on each of the grounds specified above that establishes a substantial new question of patentability.

Requester authorizes the Director to charge any fees not already provided with this request that are determined to be required to Deposit Account No. 18-1260.

Respectfully submitted,

/ Jeffrey P. Kushan /
Jeffrey P. Kushan
Registration No. 43,401

SIDLEY AUSTIN LLP
1501 K Street, N.W
Washington, D.C. 20005

Date: July 10, 2011