

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:

VINCENT R. SCARALATA

Application No.:

Filed:

For: METHOD AND APPARATUS FOR REMOTELY PROVISIONING  
SOFTWARE-BASED SECURITY COPROCESSORS

Art Group:

Examiner:

**INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §1.97**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

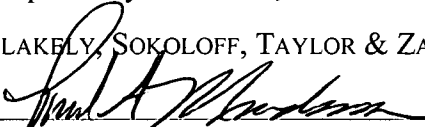
In accordance with the duty of disclosure, enclosed is a copy of IDS Citation Form PTO/SB/08 or PTO-1449, together with copies of the documents cited on that form, except for copies not required to be submitted (e.g., copies of U.S. patents and U.S. published patent applications need not be enclosed). This IDS and IDS Citation Form are being submitted concurrently with the Utility Application. It is respectfully requested that the cited references be considered and that the enclosed copy of PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

The submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made in the subject application and is not to be construed as an admission that the information cited in this statement is material to patentability.

Please charge any fees due to Deposit Account 02-2666. A duplicate copy of the Fee Transmittal (PTO/SB/17) is enclosed for this purpose.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

  
Paul A. Mendonsa, Reg. No. 42,879

Date: June 29, 2005

12400 Wilshire Boulevard, 7th Floor  
Los Angeles, CA 90025  
Telephone: (503) 439-8778

---

*Gayle Bekish*

*Date*

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E

Substitute for form 1449A/PTO				<b>Complete if Known</b>	
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>				Application Number	
				Filing Date	
				First Named Inventor Vincent R. Scaralata	
				Art Unit	
				Examiner Name	
Sheet	2	of	3	Attorney Docket Number 42P21494	

NON PATENT LITERATURE DOCUMENTS				
Examiner Initials*	Cite No.¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T²	
		P21493 - Method and Apparatus for Migrating Software-Based Security Coprocessors INVENTORS: Vincent R. Scarlata Carlos V. Rozas		
		P21495 - Method and Apparatus for Generating Endorsement Credentials for Software-Based Security Coprocessors INVENTORS: Vincent R. Scarlata Willard M. Wiseman		
		P21652 - Method and Apparatus for Providing Software-Based Security Coprocessors INVENTORS: Vincent R. Scarlata Carlos V. Rozas		
		<a href="http://www.prosec.rub.de/trusted_grub.html">http://www.prosec.rub.de/trusted_grub.html</a> - "Trusted grub"		
		<a href="http://www.vmware.com/news/releases/ace_announce.html">http://www.vmware.com/news/releases/ace_announce.html</a> - "VMware Reinvents Enterprise Desktop Management and Security with Breakthrough New Product"		
		<a href="http://www.cl.cam.ac.uk/Research/SRG/netos/papers/2003-xensosp.pdf">http://www.cl.cam.ac.uk/Research/SRG/netos/papers/2003-xensosp.pdf</a> - "Xen and the Art of Virtualization"		
		<a href="http://www.eecs.umich.edu/CoVirt/papers/revirt.pdf">http://www.eecs.umich.edu/CoVirt/papers/revirt.pdf</a> - "ReVirt: Enabling Intrusion Analysis through Virtual-Machine Logging and Replay"		
		<a href="http://ieeexplore.ieee.org/iel5/2/20660/00955100.pdf?arnumber=955100">http://ieeexplore.ieee.org/iel5/2/20660/00955100.pdf?arnumber=955100</a> - "Building the IBM 4758 Secure Coprocessor"		
		<a href="http://www.cl.cam.ac.uk/Research/SRG/netos/papers/2004-oasis-ngio.pdf">http://www.cl.cam.ac.uk/Research/SRG/netos/papers/2004-oasis-ngio.pdf</a> - "Safe Hardware Access with the Xen Virtual Machine Monitor"		
		<a href="http://www.cs.utexas.edu/~shmat/courses/cs395t_fall04/rager.pdf">http://www.cs.utexas.edu/~shmat/courses/cs395t_fall04/rager.pdf</a> - "TERRA: A Virtual Machine-Based Platform For Trusted Computing" (presentation)		
		<a href="https://www.trustedcomputinggroup.org/home">https://www.trustedcomputinggroup.org/home</a> - "What is the Trusted Computing Group?" (Internet home page)		
		<a href="http://www.cs.dartmouth.edu/~sws/papers/mswm03.pdf">http://www.cs.dartmouth.edu/~sws/papers/mswm03.pdf</a> - "Experimenting with TCPA/TCG Hardware"		
		<a href="http://www.vmware.com/pdf/TechTrendNotes.pdf">http://www.vmware.com/pdf/TechTrendNotes.pdf</a> - "NetTop: Commercial Technology in High Assurance Applications"		
		<a href="http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf">http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf</a> - "The Need for TCPA"		

Examiner Signature	/Beemnet Dada/	Date Considered	01/13/2009
--------------------	----------------	-----------------	------------

\*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication.

¹Applicant's unique citation designation number.²Applicant is to place a check mark here if English language Translation is attached.

Based on PTO/SB/08B (08-03) as modified by Blakely, Solokoff, Taylor & Zafman (wlr) 08/11/2003.  
Send To: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BD/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BD/