Title: PER-USER AND SYSTEM GRANULAR AUDIT POLICY IMPLEMENTATION

Abstract: System performance may be optimized, and extraneous audit noise reduced, by providing the capability of exercising a fine degree of control over individual audit events. A user such as an auditor interested in an individual audit event can obtain desired results without also obtaining results of all other individual audit events in the category containing the individual audit event. Additionally, audits may be obtained on either a per-user basis or on a system-wide basis. In this way, the auditor may tailor auditing events without regard to the auditing events established for other users of the system. Thus, there is a capability of establishing auditing policies for the entire system, in which case all users of the system may obtain results of the system-wide auditing.

Diagram: Diagram shows a computer with labeled components: 210 Local Security Authority (LSA), 215 Audit policy store, 300 Audit categories & subcategories, 220 Private APIs, 225 Audit-related RPC interfaces, 250 User-exposed audit APIs, 260 Per-user audit APIs, 270 System audit APIs.

Declarations under Rule 4.17:
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(U))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(H))

Published:
- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

Date of publication of the international search report: 7 June 2007

Continued on next page
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
**INTERNATIONAL SEARCH REPORT**

**A CLASSIFICATION OF SUBJECT MATTER**

IPC(8) ... PCTHelpdesk 571 272-4300
Facsimile No 571-273-3201 PCTOSP 571 272 7774
Form PCT/ISA/210 (second sheet) (April 2005)

**B FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

<table>
<thead>
<tr>
<th>IPC(8)</th>
<th>USPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>G06F 13/00 (2007 01)</td>
<td>719/318</td>
</tr>
</tbody>
</table>

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

USPC 719/313, 318, 330, 717/120, 133, 157

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Electronic data base USPTO WEST (PGPB, USPT, EPAB, JPAB), DIALOG PRO (Engineering), GOOGLE
Search Terms Used; audit, policy, event, routine, remote procedure, function etc
Date searched 05 February 2007 (05 02 2007)

**C DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 2003/0014557 A1 (BERGER et al.) 16 January 2003 (16 01 2003), [para [0006], [0019] [0037] and [0061]]</td>
<td>1-8, 19-20</td>
</tr>
</tbody>
</table>

**D** Further documents are listed in the continuation of Box C

*Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "T" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search
5 February 2007 (05 02 2007)

Date of mailing of the international search report
16 APR 2007

Name and mailing address of the ISA/US
Mail Stop PCT, Attn ISA/US, Commissioner for Patents
P. O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No 571-273-3201

Authorized officer
Lee W Young
PCTHelpdesk 571 272-4300
PCTOSP 571 272 7774

Form PCT/ISA/210 (second sheet) (April 2004)