July, 2006

TECHNICAL PRESS RELEASE

Raz-Lee Security, Inc. announces new and unique GROUP capabilities in iSecurity

1) Can you produce a report which contains only the users who have *ALLOBJ authority?

2) Can you prevent network connections between PCs which are not part of your organization?

3) Can you display the log file by groups of users defined on your system instead of (or in addition to) by the names of these users?

The era of GROUPS has arrived!

We all know that "best practices" recommends working with groups of defined users, as this simplifies all related processes- queries as well as reports.

Unfortunately, reports do not operate on the level of groups; i.e. it is not feasible to control and manage the activities which have been defined by groups, when we receive reports or information on the level of users.

Raz-Lee Security's **iSecurity** product has supported GROUPS for many years. Indeed, iSecurity supports the definition of GROUPS of users, GROUPS of IP addresses, GROUPS of device names, etc.

Now, Raz-Lee Security's iSecurity product supports GROUPS when requesting reports too!

The rule wizards incorporated into **iSecurity** have been adapted to work with GROUPS and therefore these rule wizards display all data by GROUPS, whether system groups and/or **iSecurity** defined groups. And, alongside the GROUP names appears the appropriate level of protection. One more click and **iSecurity** displays or updates the rule which is in effect.

And now Raz-Lee has designed and implemented a solution which enables defining GROUPS by GROUP-TYPES. These GROUP-TYPES can be any system entity such as files, libraries, applications, identification numbers, etc.

And, for each GROUP-TYPE, one can define an unlimited number of GROUPS and within GROUPS any number of items. For example, all identification numbers of the PCs in the organization can be defined as one group in the GROUP-TYPE defined as MACHINE_ADDRESS. Another group in MACHINE_ADDRESS may contain all identification numbers of the PCs in a sister organization.

In all comparison tables, for defining rules, for generating and selecting queries, or for defining the items in reports, the ITEM GROUP-TYPE/GROUP syntax can be used to include only those transactions which contain the GROUP-TYPE/GROUP specified. Likewise, NITEM GROUP-TYPE/GROUP can be used to include only those transactions which do not contain the GROUP-TYPE/GROUP defined.

In addition, Raz-Lee defined special GROUPS such as groups of users already defined on the system, all of which have a common identifying characteristic. For example, the group profile of the system, group profiles defined in **iSecurity FIREWALL**, and virtual groups of users named *SECADM, *SAVESYS etc. which are the users who have this particular privilege defined in their special authority.

Getting back to our original questions at the top of this document, the exception report defined in 1) above can easily be produced by defining ITEM=*ALLOBJ.

And the report defined as 2) above can be produced by defining ITEM=MACHINE_ADDRESS.

With iSecurity, the era of GROUPS has indeed arrived!

About Raz-Lee Security, Inc.
Headquartered in Nanuet, New York, Raz-Lee Security Inc. is the leading security solution provider for the IBM System i (AS/400). Drawing upon over 20 years of standard and mission-critical installation experience, Raz-Lee has leveraged vast expertise in the System i Performance and Optimization Market to design, develop and market comprehensive security solutions.

The broad scope of this experience gives Raz-Lee the insight required to develop, deploy and maintain products and solutions to assure end-to-end security for every System i configuration and application. For more information about Raz-Lee Security and its products and services, visit www.razlee.com , send an email to info@razlee.com, or call 1-888-729-5334.

###