The Clean Access Server authenticates and authorizes users from a local db or can leverage a RADIUS, LDAP, Kerberos or AD database for access information. Based upon defined policies the Clean Access Server can scan PC for such things as virus infections, port vulnerabilities, OS load, antivirus or anti-spyware, operating services and files. For non-compliant devices the Clean Access Server can isolate the devices on a per-user level and assist in network based self-remediation. Remediation methods may vary by device and supported software and may be driven by CISCO NAC partner solutions such as Anti Virus update etc.

As you are aware the amount of workload of manually managing diverse access and many diverse hosts can be intimidating. A centralized management environment for device configuration, and security event reporting should be part of the corporate merger plans.

Implementing a Network Access Control solution using the Appliance model will allow you to quickly bring Trust, Identity and Threat Defense issues under control. The type of deployment method will be determined by the existing switch infrastructure. If your organization has standardized on a Cisco switching platform you will be able to leverage the intelligence built into it reducing the number of devices required and lowering the overall cost of the NAC solution. TUG

***Sam Johnston** is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at sjohnston@intesys-ncl.com. Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday December 8, 2006.*

COiN Meeting Review — September 11, 2006

By Glenn Gundermann

COiN started off the season with veteran speaker **Richard Dolewski** presenting "Conducting a Best Practices Audit of your iSeries/400". We were enlightened as well as entertained over the course of two hours at Conestoga College in Kitchener.

Richard is a certified systems integration specialist and disaster recovery planner. If you attended the session, you would know why he is the winner of numerous speaking awards at COMMON and a member of the COMMON Speaker Hall of Fame.

Practical advice was given for often-neglected tasks. One good example of this was to secure your development environment. We take great lengths to secure our production environment and often make a complete copy into development but don't take the same precautions to secure this area. Another good example is to review default passwords. For those who didn't know, IBM's SECTOOLS menu is one valuable resource with many good options. One of them is the Analyze Default Passwords and another is to look for user profiles with a user class and special authority mismatch.

Don't forget to delete those user profiles for employees not there anymore, he says. Have you heard of "profile swaps"? If you are in charge of security, you had better take care of this. Another area to review is IFS security. We store more and more information on the IFS and the default authority is *PUBLIC(*ALL).

Auditing is not only a useful tool but also a must. As a **minimum**, you'll want to audit *SECURITY, *SAVRST, *AUTFAIL, *DELETE, *CREATE, and *SERVICE, plus everything QSECOFR and other *ALLOBJ users do. You should have exit points monitoring access for FTP, ODBC, etc.

Various best practices were covered including LPAR/HMC, backup & recovery, testing, plus others, with detailed points on each topic.

COiN speaker Richard Dolewski

"Boom is Bad!"

What I really enjoy from listening to Richard speak is his real-life experiences. We heard several stories including a customer in Mexico who finally agreed to going with a High Availability (HA) solution. This was his "Boom is Bad" story and demonstrated that different customers have different reasons for doing something. So whether you are located right beside another company that goes "Boom!" three times a year, or you want to eliminate your planned downtime from backups, it doesn't matter. Both are good reasons for HA.

Suffice it to say, it was a great session.

In summary, it's worth the drive to Kitchener to catch a COiN meeting! *

Richard Dolewski is VP of the Technical and Contingency services provided by Mid-Range, and can be reached at rdolewski@midrange.ca.

Eveline Gaede says, "Come on out for another great year of networking and learning!". COiN's next session on Nov. 6 is a two-part session on SOA. For more information, contact coininfo@coinusergroup.ca. TUG

Glenn Gundermann *is a TUG board member and chairs the TEC '007 committee. He can be reached at ggundermann@tug.ca.*

* Tug members are free to attend COiN meetings.