CHINA

Security solution used in online auditing in China

The authority on IT Audit in China described the targets of the Golden Auditing Project as the "three transformations": from post audit to a combination of post audit and concurrent audit; from static audit to a combination of static and mobile audit; and from field audit to a combination of field and remote audit. Online is not only the basic IT environment under which CNAO conducts its audit work but also the cut-in point for the audit organisation to improve its supervision. CNAO regards online auditing as an important way to achieve the "three transformations" and is doing active research. Already the CNAO has used online auditing for the Central Government Budget Implementation Audit, Social Insurance Audit and Taxation Collection and Supervision Audit.

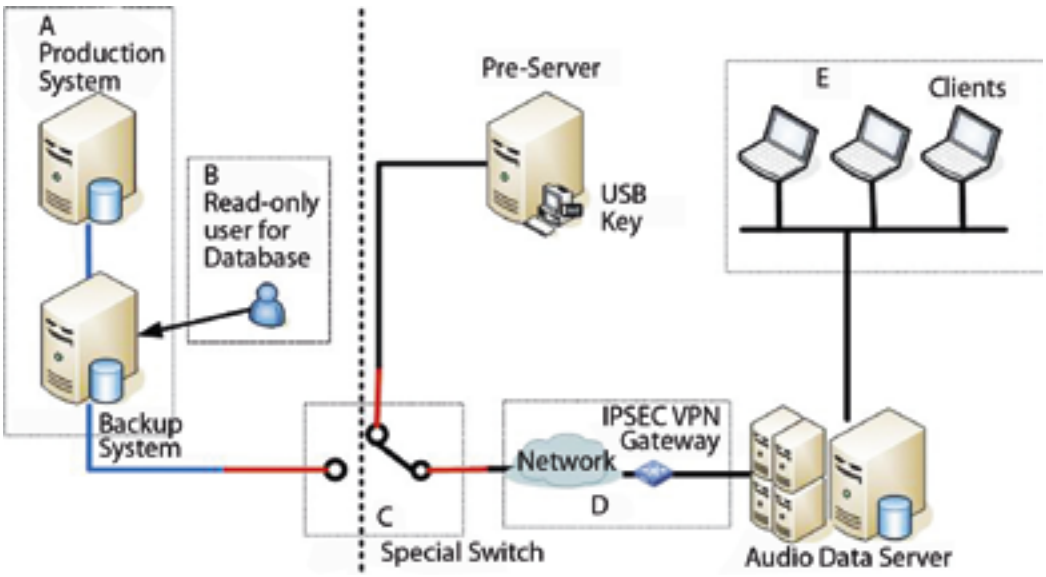
The CNAO pays much attention to security issues in online auditing and applied for a project from the Ministry of Science and Technology of People's Republic of China (abbreviates as MOST) in 2003 which MOST approved. Over three years, specialists from Tsinghua University, Harbin Institute of Technology and Nanjing Audit University took part in the research on security issues in online auditing (see Picture 1).

Picture 1: the cover of the Research Report

Based on the results of the research and the implementation of the online auditing project, the following five issues are considered to solve the security problems:

- Firstly, the audit team does not connect to the client's production system. The clients which are selected by CNAO for online auditing usually have large scale information systems for economic management and business. CNAO connects to the backup system instead of the production system. In this way, the risk of interrupting normal operations is greatly reduced and the concerns of the client about their data security are also eliminated. Furthermore, it makes online auditing easier to carry out.
- Secondly, collect the backup data with read only privilege. Because backup data is very important for rebuilding systems when disaster happens, CNAO does not perform operations such as select, filter and data mining directly on backup data. The audit team usually collects the data with read only privilege which is provided by the Database Management System such as DB2, Oracle and SQL Server. In this way the auditors cannot accidentally modify the data. The collected data is

Picture 2: Online Auditing System



stored in the pre-server, which is housed in the client's office but owned by CNAO. So online auditing will not affect the system restoration. (Part B in Picture 2).

- Thirdly, keep data separation between the client and the audit team. This can be achieved in two ways; one is to put a Pre-server between the client's system and the audit team's. The collected data is stored in this server instead of the servers in CNAO. Another is to use a special switch to keep only one route live at any one time. When the Pre-server is connected to the client, it is not accessible to the audit team. While the Pre-server is connected to the audit team, it is not accessible to the client. This avoids any direct access between the two systems. The special switch was developed jointly by CNAO and Tsinghua University. Because of the security techniques it uses, the research team has applied for a patent. (Part C in Picture 2).
- Fourthly, make the transportation safe with IP Sec VPN. According to the rules, after the data collection by the Pre-server, the Pre-server is isolated from the client and begins to transfer the data to CNAO, using IPSec VPN[1]. As well as establishing a tunnel through the public network, IPSec VPN integrates techniques such as encryption, authority and key management, so it can meet our demands for verification, authorisation, audit, integrity and confidence. (Part D in Picture 2).
- Finally, only the authorised auditors can access the data. After the data is transferred into the audit data server, auditors can analyse it with their computers. It is required that only authorised auditors should access the data depending on their assigned privileges. (Part E in Picture 2).

Using the above five kinds of measures, the data can be securely used by both the client and the audit team. The security solution is based on the following three assumptions:

1. The systems of both the client and CNAO are trusted, but the two systems should be separated;
2. The public network between the client and CNAO is not trusted and additional security measures are needed;
3. The application systems within CNAO are trusted, but should also be separated logically in order to distinguish responsibility.

WANG Zhiyu, Director General, IT Centre of CNAO
WANG graduated from Zhengzhou University of China and was awarded a Bachelor degree in Economics in 1981. He was appointed as the Director General of CNAO's IT Center in 1999. As a CIO, at present he is responsible for the implementation of Golden Auditing Project. Because of his excellent work, he was awarded the Prize of Outstanding Contributor for Promoting IT Application in China in 2004.

1 According to the US National Institute for Standards and Technology, IPsec is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control, typically used to create a virtual private network (VPN). A VPN is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks. VPNs are used most often to protect communications carried over public networks such as the Internet.