STATISTICAL COMMISSION and
ECONOMIC COMMISSION FOR EUROPE

Working Paper No. 11
English only

CONFERENCE OF EUROPEAN STATISTICIANS

Joint UNECE/EUROSTAT Work Session on Electronic Data Reporting
(Geneva, Switzerland, 13-15 February 2002)

Topic (ii): Security, confidentiality and privacy issues

USING A NEW SOLUTION FOR INTERACTIVE COMMUNICATION BETWEEN THE TWO PHYSICALLY SEPARATED NETWORKS IN THE CENTRAL BUREAU OF STATISTICS, ISRAEL

Submitted by the Central Bureau of Statistics, Israel[1]

Invited paper

ABSTRACT

The Israel Central Bureau of Statistics (CBS) maintains the concept of physical separation between the internal and external networks as a basic element in the information security policy. The CAPI (Computer Assisted Personal Interviewing) system that we use for collecting data was one of the triggers for developing an elegant method for bi-directional interactive communication between the interviewers and the organization. The Internet was the transmission channel we used, taking security problems into account. Another trigger was the inefficient process of using the two separate networks, specifically the need to transfer data between them. The solution was found using E-Gap technology. This technology is based on the Whale communications system, adapted with some additional sophisticated applications for Israel CBS specific requirements. In general, the technology which is based on the e-Gap system enables secure transfer of data in real time between disconnected networks.

I. INTRODUCTION

1. According to the statistical law in Israel, every person so requested by the Government Statistician or any empowered employee is required to answer every question in full. At the same time statistical information must be kept confidential if it either directly or indirectly enables individuals or enterprises to be identified.

2. On the other hand, the CBS also has to publish statistical information that should be available to the public but is based on this confidential data. The publications should include only aggregate records or compiled records so that the individuals remain anonymous [1].

3. Thus, because of the above, and because information is the core of business of the Bureau of Statistics, great importance is placed on data security. Security measures are very strict; they protect registers from misuse by preventing unauthorized persons from accessing information about individuals or enterprises.

4. Until 1999 the CBS in Israel maintained the best security for keeping outsiders from accessing the sensitive and concealed database. This was simple because there was no direct communication

[1] Prepared by Shifra Har and Manor Niza.

between the organization and the Internet. The web was a standalone server and was not connected to the organization network.

5. There was another identical server inside the organization (Intranet) that was used for collecting all the information that had to be published. Also used as a backup, it could replace the web hardware if necessary. In order to update the web, data on various media was manually transferred, but only by authorized personnel.

II. THE DEVELOPMENT OF THE SECURITY SYSTEMS

6. In late 1999, the CBS moved to a new and modern building, creating a unique opportunity to upgrade the entire system. One of the upgraded systems was the communication infrastructure; this update was the major catalyst to update the entire security system. The new communication infrastructure was therefore developed with the ability to integrate the advanced security system. Programming started at that time but has since improved significantly. Among all the other long-term decisions made at that time, two related to security:

- The CBS must preserve the highest security level, above the standard procedures required by law. The decision to keep individual or enterprise records highly secure (again beyond the procedures required by law) was crucial, since information is the core of the Bureau's business and the database must be confidential according to the statistical law (as mentioned above). This is a direct result of the special awareness of secret and sensitive information in Israel, the result of the long period served by most of the population in the Israeli army. Only cooperation by the public based on trust, voluntarily giving the required information, leads to the high level of proficiency of the Israel CBS publications and results in the beneficial microdata for outside researchers as well[2].

- The security system should continue on the basis of a physical separation between inner and outer networks. The idea that complete security was only possible under this condition has been the leading principle of the Israel CBS over the years.

7. This meant that the communication infrastructure should be two physically separated networks – one was the inner net (Intranet) for the ordinary processing work of the CBS staff aside from database and other information storage, and the other was the outer net to communicate with the outside world (Internet). As a policy, the inner net is developed, giving a multitude of services, whereas the outer net is degenerated; this policy is implemented in order to be sure that the outer net, connected to the Internet, will be used by CBS' employees as little as possible.

8. This physical separation requires administration that is based on manual interactive transfer of information between the two networks with a mobile medium by authorized personnel only. Although it was the best security achievable and was very useful in the past, it is no longer valid as it has become inefficient and cumbersome. In addition to the maintenance of two different and separate networks, the cumbersome manual operation is becoming more and more difficult. Public awareness of open information is responsible for the vast interest in the ICBS publications available on the CBS website shown by businessmen, administrators, and ordinary citizens alike. No longer limited to the queries of a few researchers, statisticians or institutions, there are enormous numbers of queries every day which brings the total number of visits to the website to more than 450,000 per month (the website hosts about 5,000 HTML pages, 10,000 Time Serial Analysis, press releases, and other publications). Instead of upgrading to a more efficient system in order to fulfil all the requests, the Israel CBS employees have to work on two separate parallel networks, manoeuvring between them with mobile media, since the two networks do not communicate directly in any way. Such a protocol is quite cumbersome. For example:

---

[2] Gidon Burshtein, Administration and policy of statistical data confidentiality in Israel, 1999.

- The Israel CBS researcher researching information on the Internet or who wants to communicate with colleagues outside the organization has to first use the outer network to download all the required files on a mobile medium (i.e. a diskette). Then he has to transfer these files to a special check station for scanning against viruses or other malicious programs. Finally, only after checking is completed and permission is received, can he finally use the new information for his own purposes in the inner network.

- On the other hand, to communicate with colleagues outside the Israel CBS, the opposite procedure must be carried out. First, the employee must download the selected information from the inner network server to a mobile medium. With the authorisation of the department manager, he then takes these files manually to the check station to request additional authorized permission from the particular person who is in charge of security. Only then can the information be delivered.

9. So it is clear that two physically separate networks lead to double infrastructures. From the technological standpoint, this means two control systems, double maintenance, two PC's for each user or alternatively 2in1 PC technology. The latter technology involves a complete split of the hard disc into two physically separated discs, each with its own communication card. With two separate communication cards, each one of these two discs is connected to a different network; either to the Intranet (LAN) or to the outer network connected to the Internet. Every transfer procedure from one network to the other, using the 2in1 PC technology, requires an additional computer boot. This technology does possess the possibility of an interface zone between the two networks, to allow information to pass from one network to the other, but it allows only one selected direction that must be determined before the program is installed. This is not a common procedure in organizations, and is not recommended.

10. In late 1999, under the new communication infrastructure planning and reconstruction, the decision was made to seek out a new method to pass information between the inner and outer networks interactively; something that would incorporate the architecture of two networks unified into one. It was accepted that indirect manual communication between two disconnected networks was insufficient and for all intents and purposes, impossible. The enormous updating of data that must be transferred between the networks increases exponentially and requires a novel solution. The solution, of course, must also meet the requirements of a very sophisticated security system, befitting the CBS Israel restrictions.

11. Additionally, there has been a great advance in data collection systems, and one of them, the CAPI (computer assisted personal interviewing) technology, is being widely applied in Israel CBS. This technology was one of the catalysts in the development of bi-directional interactive communication in the ICBS, and the Internet was accepted as the means of bi-directional information exchange between the interviewer and the center. Bi-directional communication through the Internet exposes the organization to some new outside risks that did not exist before. This, of course, now requires special consideration in the whole information security context.

12. We should also be aware of two additional security problems:

- Using the insecure Internet as a transmission channel to transfer sensitive collected data to a server within the outer network;
- Storing this exposed sensitive information for a relatively long time in the outer network until the transfer can take place manually (even if, in reality, it is for a short time).

13. Interactive direct communication with sensitive data is a threat to security and secrecy. The security system is not entirely protective, even if the website is modern, protected by the best firewall, the information is encrypted, and access is permitted for authorized persons only.

14. In the CAPI [2] system the interviewer communicates with the CBS database server in bi-directional interaction via the Internet: interviewers from all over the country send their data collection directly to the central data base server by way of the Internet; and they receive feedback including the follow-up portions of questionnaires in order to continue. This daily interactive operation is a crucial condition for working with the LAPTOP in the field. Otherwise, without follow-ups and updates, the method becomes inefficient. This way, the method allows the data to be quickly available to the employees in charge of control and overseeing of the work. The collected data should be sent as soon as possible to the center and erased from the LAPTOP in order to minimize their time duration outside the secured Intranet. The interviewer automatically and continuously receives new questionnaires from the secured server within all administrations concerned, old ones with mistakes (for re-interviewing), as well as feedback for other work.

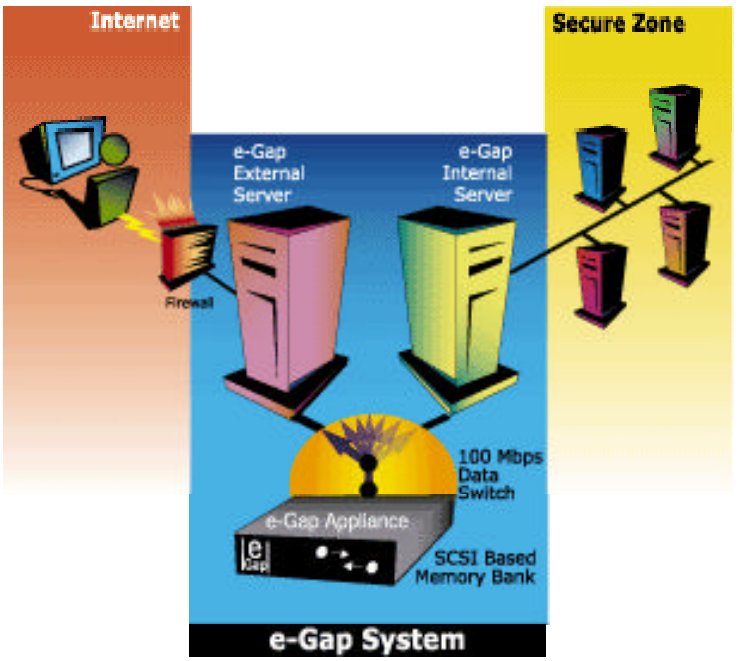
III. THE NEW CBS ISRAEL SECURITY SYSTEM

15. The resulting decision was to preserve the physical separation concept, i.e. to find a method that enables the two networks to communicate and yet keep the physical separation architecture. As mentioned before, while planning the new network infrastructure, the sophisticated new security system, in which the principals were already developed (at that time), was taken into consideration. Therefore, the infrastructure was constructed in such a way that today it is relatively easy to integrate the new security system for immediate use.

16. We can learn how the sophisticated system actually works by using the CAPI as an example. From a security standpoint, the CAPI is one of the most problematic communication operations, since it represents all the various contacts that may be carried out on the network infrastructure. Below follows a description of the solution to manoeuvre between the two physical networks:

17. The solution to the security problem is the Air Gap Technology based on the Whale communications [3] technologies and adapted to the CBS Israel specific requirements with some additional sophisticated applications. In general, the idea is to connect the two networks (the Internet and the Intranet) but not at the same time, in order to preserve the physical separation between them, which means OFF LINE communication. Although the technology is used in offline communication mode, it does allow transfer of data into the inner net, and at the same time prevents the secure data from staying in the outer network for any longer than necessary.

Figure 1: e-Gap System never connects the two networks together



18. The e-Gap System is a hardware and software solution comprised of three elements:

i) The external server - connected to the outside world;
ii) A second server (the internal server) - connected to the secure zone;
iii) The solid state e-Gap appliance - connected between two servers.

19. The solution is a method based on two servers and one disc. The first server is computer EEX called e-Gap External Server. The second server is computer EIN called e-Gap Internal Server. The DISC called e-Gap is an appliance located between the two, connecting the two servers, which serves as an interface zone (Figure 1). The EEX is part of the Internet network as an outer server and the EIN is part of the Intranet. There is only one connection for the DISC appliance which either links to the EEX (to the Internet) or to the EIN (to the inner LAN) in a fixed frequency (never to both), and shuttles files between them.

20. Every bit of information that comes from the Internet enters computer EEX and then is checked by the security system for permission. This permission lets the server connect with the interfaced disc according to the fixed frequency, transfers the information from the EEX server to the disc and then erases it. Then, according to the same fixed frequency, the alternative connection exchange from the disc to the EIN server takes place. The information passed from the disc EIN server is checked there a second time by another security system with some other protection means for permission. This permission then lets the information pass to a third special computer within the inner LAN, the dedicated web collecting server, and only then is it available for the CBS Israel staff. This third computer differs from any other general servers in that it can not be used for any independent operation or application. This serves a great advantage because it can be operated only by the other computers in the Intranet and only for releasing information or sending information, not actually processing anything. This technology, with the addition of the procedure not to use the third server as a standard server, is responsible for more efficient security and excellent protection. The interfaced disk, meanwhile, disconnects from the EIN server and reconnects to the first computer again to start a new cycle of information delivery from the outer network into the Intranet via the e-Gap technology.

IV. CONCLUSION

21. The security system, consisting of two physically separated networks, is a safe model but it is inefficient, since the demand is for much more sophisticated data administration. Operations like data collection, data management, data processing and information manipulation are supposed to be carried out automatically via Internet which is combined with the organization Intranet, and cannot be accomplished manually any longer. The vast usage by either researchers or ordinary users on one side and their awareness of information security on the other side requires creative protocols for both a secured and comfortable working environment.

22. Described above is one option for a secured and efficient working system. This technology enables easy update to the Israel CBS web site. The interviewers can use the CAPI system to communicate with the center “directly” via Internet and CBS can use the CAWI (Computer Assisted Web Interview) system in a simple way as well. In all three cases, the security system is a device that transfers data between two physical networks.

REFERENCES

1. Gidon Burshtein, Administration and policy of statistical data confidentiality in Israel , 1999.
2. Hide Degerdal, The process of making a new CAI operation in statistics Norway, 2000.
3. Whale communications, Air-gap Technology for E-business, 2001.