

Visions from the IT Engine Room

TC-11 Security and Protection in Information Processing Systems

Interview with Leon Strous, TC-11 Chair (May 2001 - May 2004)

Leon Strous is senior IT-auditor in the Payment Systems Policy Department of De Nederlandsche Bank (DNB), the central bank of the Netherlands in Amsterdam. Together with his colleagues he assesses the security and reliability of payment systems and payment products. He is also involved in work in this area done by the European System of Central Banks (ESCB). Prior to joining DNB in 1993 he has worked for Philips Electronics since 1985 in the areas of internal control, administrative organization and information security. His education is in business administration and business informatics (both equivalent to a bachelor's degree) and postgraduate IT-audit at the Vrije Universiteit Amsterdam. He is a registered IT-auditor (RE) in the Netherlands and a Certified Information Systems Auditor (CISA).

His IFIP involvement started in 1993 as the vice-chair of the organizing committee for IFIP SEC'94. He is the Dutch TC-11 representative since 1994 and the chair of this committee since May 2001. He has been the chair of working group 11.5 from 1996 until 2001. He is also the GA member for the Netherlands since 2001 and a member of the WITFOR Steering Committee.

His other activities include the vice-presidency of the Dutch Computer Society (NGI) since 2000 and the membership of standards committee 381.27 Security techniques of NEN (the Dutch national standards body) since 1993. Besides information security, due to a lack of time his hobbies are limited to an occasional game of squash and billiards.

The Delivery Co: In your opinion, which are the most significant developments and activities of your TC since its foundation?

L. Strous: although according to the records TC-11 was formally established in 1984, the first IFIP SEC conference (TC-11's flagship conference) already took place in May 1983 in Stockholm, Sweden. The early eighties were the years when personal computers started to invade people's lives. We saw an increasing concern about several issues like privacy and we witnessed the "birth" of computer viruses. The attention for security started to evolve from the closed defense and mainframe environments to business and small computer environments, from confidentiality towards integrity, from technical security to managerial issues. This was clearly an era where establishing a TC dedicated to security was an obvious thing to do. The founders made it clear by the name and aims and scope of TC-11 that security is not limited to computers but encompasses computers, applications, data and the organization. That was more or less a visionary view because in those days the term computer security was more common than the term information security.

The activities of TC-11 have always followed the developments in our field and it has been a contribution of TC-11 that all aspects of security have been broadly covered at its SEC conferences, with attention for new developments and new concerns. The working groups address a wide area of more focused topics in their working conferences: information security management, small systems security, data and applications security (previously database security), communication and network security, integrity and internal control in information systems, IT misuse and the law and security education. Through its conferences and working groups, TC-11 has succeeded in pursuing its aims and scope to increase the reliability and general confidence in information processing, to act as a forum for security managers and other professionally active in the field of information processing security, to disseminate information and exchange practical experience in security work and to promote security and protection as essential elements of information processing systems.

An important achievement of TC-11 has been the drafting of two statements that have been adopted by IFIP. The first statement concerns IFIP's position on cryptopolices and this was drafted in the second half

of the nineties when cryptography was a hot topic from a policy point of view and discussions concentrated on questions such as whether governments should have access to the keys in encryption systems used by companies and individuals. A second statement concerned information security assessment and certification and addressed TC-11's opinion that the information security status of IT systems and the information security management of such systems should be assessed against specified standards related to information security management and that members of IFIP should be instrumental to ensure that such standards, for systems and individuals, be harmonized on an international level. Last year, TC-11 agreed on another statement which contains a request to all member societies of IFIP to urge their relevant government and education bodies to ensure that proper education and certification requirements are set for those people who intend to become information technology security professionals and including those who audit the security of IT systems. In my view such statements are important contributions to the information society and IFIP should issue such statements timely whenever there is an opportunity.

Another achievement concerns the objective to promote security and protection as essential elements of information processing systems. TC-11 has been successful in this area, which can be measured directly within the IFIP community by the fact that more and more TC's and working groups are including security in their aims and scopes. I am particularly pleased with the increasing cooperation between TC's and working groups on security topics. Good examples of this are the Communications and Multimedia Security (CMS) conferences of TC-6 and TC-11 and the E-Commerce, E-Government and E-Business (I3E) conferences of TC-6, TC-8 and TC-11. And of course I must mention the joint working group with TC-9 on legal, privacy and social issues (Wg 9.6/11.7 IT: Misuse and the Law), a very successful example of an active cooperation. I am confident that such cooperation will only increase in the near future.

The Delivery Co: Are there any current technical activities within the scope of your TC, which you feel could have a significant societal/economic impact in the future?

L. Strous: The most obvious issues that already have a significant impact are cyberterrorism and (critical) infrastructure protection. Not only do these issues require new technologies or larger scale use of known technologies such as biometrics and smart(er) cards, but they also shed a different light on privacy issues and human aspects as was already mentioned by Jacques Berleur in his TC-9 vision. To address these issues in an effective way requires even more cooperation between the different IFIP disciplines than I described previously. Probably most of the TC's will or should be involved, just think of topics like software quality (TC-2), training people (TC-3), safety-critical systems (TC-10), social aspects and human-computer interaction (TC-9 and TC-13). It will be a challenge for the IFIP community to define projects that result in meaningful statements, guidelines and tools that can be used by many interested parties, rather than only discuss research results and business practices between the professionals within our own community.

Trust and confidence in the security and reliability of all the "e-words" is something that is necessary for all these e-words to become the success that everybody is hoping (and waiting) for. In my view many of these e-words are just buzzwords, it seems like everything from our "old" world is being e-d. However, there is no doubt that some of these areas already have or most certainly will have a significant impact on our society. This means that many topics within the scope of TC-11 are influential in that respect. Just think of identification and authentication means (biometrics and smarter cards again?), integrity of messages, secure business transactions and payments, and so on.

Another remarkable observation is the fact that some old issues have not disappeared and that we have not succeeded in eliminating them. Although their "hot" days are over and they are no longer in the focus of attention (with the exception of an occasional short hype), these activities still have and will undoubtedly remain to have a significant impact. Hackers and viruses continue to cost our society a lot of money and the security professionals must keep trying to find ways to limit the effects as much as possible.

The Delivery Co: Are there any specific technical issues you find important for IFIP as a whole to address?

L. Strous: As said before, issues like cyberterrorism and critical infrastructure protection may require a broad IFIP involvement. And although these issues may seem to be of a technical nature, we cannot hide from the fact that cultural and political aspects also do play a role. IFIP must take this into consideration when addressing these issues and must try to find a way to deal with it as “neutral” as possible.

Another important issue is attention for developing countries, a view shared with many of my fellow TC-chairs. It is good to see that IFIP fully supports the work of the Developing Countries Support Committee (DCSC) and the World IT Forum (WITFOR). Discussions during the preparation of the first WITFOR conference (to take place in August 2003) have shown that IFIP should evaluate the approach towards developing countries and should address the questions whether the old (western) attitude is still valid and whether the old approach is still the most effective.

A final issue I would like to mention concerns fundamental research. In economic downturns, there is a tendency in industry to only spend money on work that shows immediate practical results / products. I guess that this is not only the case for security research but for all IT aspects and areas. IFIP should make it clear to industry and perhaps also to governments that (theoretical / fundamental) research is necessary and often lead to discoveries of useful tools and means, that perhaps would not have been discovered had research only been driven by direct (industry) needs.