The reports about security weaknesses in ICT and the Internet and the subsequent discussions about trust mechanisms and trusted parties have motivated IFIP to issue a statement on the topic. IFIP with its diverse international structure of around 50 member societies is not the body that issues statements on current issues lightheartedly, but the seriousness of the issue led to a clear statement, accepted by it's General Assembly. IFIP realizes that such a statement can only be the beginning of work on the issues and will seek cooperation between it's technical bodies and it's member societies to do this work, wherever possible also with other interested parties.

IFIP statement on intentional weakening of security and trust mechanisms in ICT and the Internet by government agencies and other major actors

2013-10-24

IFIP has followed the recent reports about security weaknesses in ICT (Information and Communication Technology) and the Internet with great concern. There is reason to believe that major practical pillars of trust in the Internet, e.g. the trustworthiness of relevant communication nodes and the security of cryptographic implementations in the web such as SSL, are being intentionally weakened in a systematic way at the behest of government organizations and other major actors in the field. This is endangering and undermining the fabric of the Internet and the Information Society, and contradicts the claim of those actors to be trusted with e.g. sensitive personal information. Moreover, any deliberately introduced weakening or backdoor is equally exploitable by (ostensibly) legitimate and illegitimate third parties alike.

We know that we do not live in a perfect world: Technology is never perfect and has too many inherent weaknesses anyway, while its complexity makes it hard to find errors and detect attacks. However, the scale and dimension of intentional weakening of ICT infrastructures and protection mechanisms by actors, who claim to be trustworthy, is astonishing and disturbing. It has undermined many trust assumptions, and has also unnecessarily endangered the security of infrastructures and systems that could be of better quality even by today's state of the art.

This means we must now be specifically critical, whenever we get answers such as “Trust us” instead of thorough and open explanations of the described attacks. The same requirement to be critical holds for any ICT functionality and assurance. Any different behavior multiplies the risk that lowering of trust in ICT and the Internet may turn into a loss of trust in the ICT profession itself.

As IFIP members and ICT professionals we know that we will need to be more critical, and to work harder for steps towards the goal of ICT systems that users can safely trust in with the protection of their data. Based on experience the most important aspects are:

- A stop on government-sponsored measures that are intentionally weakening the security mechanism of ICT and internet technologies;
- Open and frank descriptions, explanations, and discussions of current and future weaknesses, e.g. on the steps that have been taken to prevent illegitimate exploitation, and a pause, while the implications of the weaknesses become better understood;
- An open trust infrastructure, that resists domination by major players;

- Transparency of ICT and the related infrastructures and operation procedures, e.g. if the risk calculation employed says that the cost of the increase in fraud is worth the increase in security;
- Implementation of protection mechanisms that users can really control;
- An infrastructure of independent institutions to assess the security and reliability of complex ICT.

Interested parties are invited to get in touch with IFIP (ifip@ifip.org).