Keynote:

About the Role of IT Security in the Information Society

Klaus Brunnstein

Faculty for Informatics, University of Hamburg, Germany
International Federation for Information Processing (IFIP), (Past) President
brunnstein@informatik.uni-hamburg.de

Paper presented at the **3rd International Conference on IT-Incident Management & IT-Forensics (IMF 2007) Stuttgart, Germany (September 11 - 13, 2007)**

Abstract: The development of economies, national and international organisations as well as of many aspects of social and individual lives are growingly determined by developments of Information and Communication Technologies (ICTs). Consequently, institutions, governments and many scientists refer to the actual phase of human history as shaping an **"Information Society" (IS)** (or "Knowledge Society", as named by UNESCO and other UN organisations). Developments are much faster than in the **"Industrial Society",** but there are surprising similarities which may best be described in analogy to the theory of **economic cycles** of the Industrial Society, developed by Schumpeter and Kondratieff. Locating the start of the Information Society about 1940 (with first computers such as Zuse Z3 and ENIAC), the **first "IS cycle"** – comparable to steam engines following James Watt´s invention, is determined by single computers with initially very low capacities but fast improvement in speed and storage together with reduction in space (micro-miniaturisation). Comparable to the development of traffic networks (railways etc) in the Industrial Society, single computers are interconnected in the **second IS cycle** to form networks of growing complexity, with software technologies developing autonomous agents to support system and application work.

As experienced also in the Industrial Society, **InSecurity** governs the first and second phase of the Information Society, and networks (esp. The Internet) and computer systems (whether clients or servers) are as "Insecure and Unsafe at any speed" (quoting Ralph Nader) as industrial products in related phases. Besides many beneficial effects of IT for enterprises, organisations and individual, many incidents have contributed to significant loss and damage. Even pubertarian boys succeed easily in attacking important IT systems and produce significant damage to systems, users and customers.

Causes for IT InSecurity are manifold, ranging from paradigmatic to practical aspects. Among several reasons, including basic design of technologies, IT experts do not care sufficiently for the consequences of their design, products and usage. As technical improvements of contemporary IT systems will - for a foreseeable period - only partly help to overcome basic causes of InSecurity, education of IT engineers to safer and more secure design and implementation of their products may help to reduce IT risks. While some professional organisations such have suggested some rules for ethical behaviour of their members, contemporary curricula fail to include Ethics into the education of IT experts esp. including System and Software Engineering. Consequently, reduction of InSecurity must address all related aspects.

"Good Practice" becomes more important with growing dependency of enterprises, organisations, governments and individuals on vulnerable, interconnected IT systems, IT (through improved methods and protocols) and legal experts (also through internationally accepted rules) must find **ways to reduce contemporary InSecurity**.