Cyber Systems Security

We identify, explore and use ideas, concepts, and models in order to protect the value of the information, which is stored, processed and transmitted by various digital systems. While the technology solves some of the problems, it also opens new ones such as unlawful behaviour, which amounts to fraud and forgery, theft, pornography, cyber terrorism and cyber warfare. The research in this area ranges from mathematical modelling, artificial intelligence methods, heuristics and protocols, to social, psychological and economic theories to understand, explain, predict, control, and generate any type of security systems. The goal is to research and create dynamic systems for curation and management of security and privacy that would increase the overall resilience and trustworthiness of the global knowledge space, and prevent the informational meltdown of the contemporary e-Society and the universal digital eco system.

Security for the Digital World

A vast number of social, economic, political, cultural, scientific, educational and even entertaining services, which are essential to the contemporary society, are either already or are going to be created on line. The omnipresent local, national or global digital systems that generate a transcendent service space depend on technologies, policies, regulatory settings, economic and political interests, social relevance, human knowledge and boredom.

Obviously, in these highly dynamic environments quite often termed as digital societies, "where everything is a service and service is everything", the design, implementation, adoption and use of secure, resilient, privacy aware and trustworthy technological and social infrastructure, simply means a difference between a functioning and a non-functional world.

With information services being ubiquitous, mobility implied, and availability assumed, information accountability and responsibility, as well as transparency are vital attributes of the comprehensive approach to the research in security, privacy, trust, and assurance. The work draws on general systems (both artificial and living) theory, psychology and sociology of communication, various management concepts, decision and risk analysis, algorithms for manipulating large volumes of data, software engineering, design and implementation of resilient and reliable e-Infrastructures including Internet of things and clouds, producing and preserving the integrity of digital evidence to keep the digital world safe and amicable, and preparing for the challenges such as any Internet scale events, that include massive distributed cyber attacks, black-outs and dark nets.

In addition, the research should discover models for identifying and analysing digital evidence, and protocols for digital forensics that will enforce the salient features of accountability and yet protect privacy from various sources of data mining activities that should undeniably be subject to legal framework. Moreover, the emergence of Internet and network forensics should produce procedures and tools that work beyond discovery of irregularities. In other words, they should create systems for real time control of security and privacy that should increase the overall resilience and trustworthiness of the information space.

Contacts

Oliver Popov
Fredrik Björk

Please consult the weblink for contact information.

Ongoing projects

STORK 2.0

Future learn: SLL

eSens

Department of Computer and Systems Science, DSV
www.dsv.su.se/security

Stockholm University