Designing Digitall Responsible System, Software and Services

William J. Yeager
Retired
Knowledge Systems Laboratory, Stanford University
byeager@fastmail.fm

Jean-Henry Morin
Institute of Information Service Science
University of Geneva, Switzerland
Jean-Henry.Morin@unige.ch

Vince Cerf and Tim Berners-Lee recently stated, "The Internet is a disaster." What did they mean by this? While there are physical layer problems, these are infrequent, resolvable, and, in our opinion, not part of this "disaster." They are also not referring to the IETF and W3C protocol standards. Rather, a significant part of the major, ongoing problems that have led to this disaster result from companies' digitally irresponsible system, software, services design and engineering enabled by executive, management decisions. These companies then benefit from billions of dollars of annual revenue generated by their users.

The Internet disaster is multi-faceted. Two salient facets among the many are: The exponential growth this decade has resulted in billions of dollars of losses; the exploitation and at times illegal use of billions of users' personal data as well as the violation of their privacy for the purpose of generating revenue.

The goal of this Minitrack is to address possible solutions that will enable the users to take control of their digital fate or at least ensure that "by design" system and service providers address such digital sustainability goals which are at the heart of a digitally responsible society.

To this end we have the following three papers:

Because identity management is critical in any digitally responsible system design, technical as well as non-technical assumptions are equally important. The first paper, "The Review of Non-Technical Assumptions in Digital Identity Architectures," by Anar Bazarhanova of Aalto University, and Kari Smolandaer of LUT University, report an overview of the current research in digital identity management. To accomplish the latter a systematic literature review of digital identity solution architectures was done to extract the inherent non-technical assumptions.

Securing IoT devices or embedded systems, which do not support double-precision-floating point arithmetic, requires novel cryptographic approaches. Its importance is part of the bed rock of the goals of this Minitrack. The authors, Hitoyaki Yoshida, and Haruka Fukuchi of Iwate University in their paper, "Implementation of High-Speed Pseudo-Random-Number-Generator with Chaotic and Random Neural Networks," present such an approach.

Since the late 1970's, the Internet IETF RFC process has produced standards that are extremely well vetted in working groups. With the advent of the WWW, many vendors have published experimental RFC's defining protocols for data transfer. They are not vetted by the IETF's standards process, and are often attackable. The authors, William M. Pitts of the Cirrus Project, and William J Yeager, retired from the Stanford University Knowledge Systems Lab, propose as a viable solution, "Cirrus: A Digitally Responsible, Global File System." This file system has been developed over several years. Cirrus' distributed shared memory implementation provides a fast and secure method of transporting all network traffic within a global, overlay networ

URI: https://hdl.handle.net/10125/64526
978-0-9981331-3-3