Networking Computers and People: Design and Evaluation

Habilitation Thesis
Summary

Răzvan Rughiniș
University POLITEHNICA of Bucharest

2014

Summary

This habilitation thesis presents our research and professional activity in the fields of networking, computer-supported collaborative learning (CSCL) and human-computer interaction (HCI), spanning a period of five years.

Daily life as well as professional activities are increasingly networked and distributed across heterogeneous systems in which humans interact with different types of devices. This rapidly increasing interconnectedness mediated through technology raises novel challenges, especially as regards security and privacy, on the one hand, and the ability to explore and engage efficiently a vast array of communication flows, on the other hand. A search for solutions involves the pursuit of technical optimizations in interaction with studies of users' experiences and actions, in order to harmonize actual practices with technical affordances.

Our recent research in the field of security involves Wireless Sensor Networks and Mobile Networks. We present the WSN Complex Security Framework, to which we have contributed in the development of five components: Authentication and Anti-Replay Security Protocol AASP; Attack and Fault Detection Framework TinyAFD; Adaptive Trust Management Protocol ATMP; Trust and Energy Aware Routing Protocol TER, and Adaptive Security Framework for Wireless Sensor Networks. These protocols improve on state-of-the-art technologies through a comprehensive coverage of risks, focus on energy-efficiency, methods of balancing conflicting requirements, and mutual integration into a comprehensive protection layer.

We have also contributed to optimizing privacy in mobile networks, aiming to support secure location queries for services such as natural disaster alerts, or other location-based alerts. Since such systems require constant location tracking, they are vulnerable to personal information misuse. Our proposed architecture is based on novel cryptographic algorithms that permit secure predicate evaluation on encrypted data. The service provider is thus able to evaluate clients' encrypted location data, with no knowledge of their exact location. Because a naïve implementation is not fast enough to support real-world applications, we propose several optimizations relating to spatial information encoding and predicate construction that improve upon the naïve baseline to obtain a scalable, efficient solution.

Our research in the CSCL and HCI fields is grounded in the theoretical insight that tools are constitutive for action, and thus we extend and shape our perceptive, cognitive, motivational abilities through information technologies. At the same time, tools are not given outside of concrete instances of use: they become tools through users' situated activity. We examine the interplay between design and situated use of information technology. Unpredictability and mutual adaptation of users and technologies are core concerns in HCI and CSCL / CSCW, and we aim to formulate user models and other design heuristics (definitions, classifications, principles) that better take into account the spontaneity of situated action and the flexibility and variability of use across and within individuals. Our studies concern three areas of interest: attending to *the imagined users* incorporated in technical systems, modeling actual use through classification analysis to identify relevant *use* and *user types*, and formulating *lessons-learned as heuristics*, based on designers' and users' experiences. Firstly, we investigated the imagined users implicit in technologies such as apps for smoking cessation or serious games for learners. Secondly, we examine the diversity of actual use for serious games and other learning and knowledge-making platforms. Thirdly, we propose design heuristics for gamified systems, including the creation of serious games for learning and the development of digital badge architectures. We rely on case studies of systems that we have coordinated or in which we have

participated as members (gamified learning platforms, online communities), in order to highlight the relevance and added value of the proposed heuristics.

Several of our research directions in the fields of network security, CSCL and HCI rely on investigations concerning platforms and initiatives with which we are closely engaged, as coordinators or members. This convergence of research and development has allowed us to reflect on our own experience of design and use, and to improve our professional activities in the academic community based on research evidence.

The second part of the thesis highlights several directions for future research. As regards security and confidentiality in the Internet of Things, we are interested in algorithm optimization: although our work shows that Hidden Vector Encryption - HVE based location services can be practical, there are still multiple challenges that need to be overcome in order to support more complex solutions. We plan to address several current limitations, in order to make possible queries that refer to distances between users and points of interest outside of the reference geographical area, to scale to larger geographical areas and predicate numbers, and possibly to leverage advantages of HVE techniques with Private Information Retrieval - PIR based systems that do not require a trusted third party.

We are also interested in empirical research on the diversity of users' cyber-security orientations, in order to create effective ways of visualising and signalling security and privacy information, enhancing risk awareness and protective skills through peer communication, and to embed best practices of end-user security in the development of the Internet of Things.

A third direction of interest for future research consists in the study of computer-supported knowledge-making systems. We are particularly interested in collaborative platforms on which device-mediated communities contribute to addressing specific problems: feedback aggregates in *reputations* in online shopping or travel sites; Q & A communities assemble *collections of experiences* to inform the asker's perspective; Wikis attempt to generate *coherent multi-authored documents* bringing together (in puzzle-like structures) information from different collaborators; publishing collectives or communities assemble *interactive exhibitions*. In such online settings, we aim to investigate how technology shapes access to diverse worldviews; how decision-making evidence is changed through access to peer experiences; and how IT tools contribute to self-understanding and self-making, through users' novel practices of self-monitoring and management. A specific project refers to the development of 'Complex Accessible Remote LAboratories for Engineering Education and Applied Research' – CARLA, to cultivate engineers' sense-making skills in system failure situations.