Interconectând Calculatoare și Oameni: Design și Evaluare

Teză de abilitare
Rezumat

Răzvan Rughiniș
Universitatea POLITEHNICA din București

2014

Rezumat

În această lucrare vom prezenta activitatea noastră de cercetare și profesională în domeniile rețelisticii, a învățării colaborative bazate pe calculator (CSCL) și a interacțiunii om-calculator (HCI), acoperind ultimii cinci ani.

Atât viața cotidiană cât și activitățile profesionale sunt în tot mai mare măsură distribuite și mediate prin sisteme tehnologice eterogene, în care oamenii interacționează cu diferite tipuri de dispozitive. Interconectarea tot mai densă ridică probleme noi – mai ales privind securitatea și confidențialitatea informațiilor, dar și privind actualizarea potențialului de explorare și folosire eficientă a fluxurilor de informații. Căutarea soluțiilor implică atât optimizări tehnice, cât și studii ale experiențelor și acțiunilor utilizatorilor, pentru a armoniza opțiunile tehnologice cu alegerile efective ale oamenilor.

Cercetările recente pe care le-am realizat în domeniul securității se referă la rețelele wireless de senzori (WSN) și la rețele mobile. În teză prezentăm soluția WSN Complex Security Framework, la care am contribuit în dezvoltarea a cinci componente: 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, și Adaptive Security Framework for Wireless Sensor Networks. Aceste protocoale îmbunătățesc nivelului de securitate state-of-the-art prin acoperirea cuprinzătoare a diversității riscurilor, prioritizarea eficienței energetice, balansarea cerințelor conflictuale și integrarea coerentă într-un sistem comprehensiv de securitate.

Am contribuit de asemenea la optimizarea confidențialității în rețelele mobile, în scopul susținerii serviciilor de prelucrare securizată a locațiilor în sisteme precum alertele pentru dezastre naturale sau alte alerte bazate pe locație. Deoarece aceste sisteme necesită o monitorizare constantă a localizării utilizatorilor, aceștia devin vulnerabili în fața utilizării malițioase sau inechitabile a informațiilor lor personale. Arhitectura pe care o propunem se bazează pe algoritmi de criptografiere care permit evaluarea securizată a predicatelor privind date encriptate. Ofertantul serviciilor este astfel capabil să evalueze date privind localizarea encriptată a clienților, fără a avea efectiv acces la poziția exactă a acestora. Am propus și o serie de optimizări în ceea ce privește encodarea informației spațiale și construcția predicatelor, îmbunătățind performanța dincolo de nivelul de bază al unei implementări naive și permițând dezvoltarea unor soluții scalabile și eficiente.

Cercetările pe care le-am realizat în domeniile CSCL și HCI sunt orientate de premisa teoretică conform căreia *instrumentele sunt constitutive acțiunii*. Prin urmare, prin tehnologiile informației ne extindem și ne modelăm capacitățile perceptive, cognitive, de motivare și autocontrol etc. În studiile realizate am examinat interrelațiile între design și utilizarea situată a tehnologiilor informației. Impredictibilitatea și adaptarea reciprocă a utilizatorilor și tehnologiilor sunt două preocupări centrale în domeniile HCI și CSCL/CSCW, pe linia cărora urmărim să formulăm *modele de utilizatori* și alte *heuristici pentru design* (definiții, clasificări, principii) care să surprindă cât mai bine spontaneitatea acțiunilor situate, flexibilitatea și variabilitatea utilizării tehnologiilor. În cercetările recente am urmărit trei arii de interes: studiul detaliat al *modelelor implicite de utilizatori („utilizatorii imaginați") ai soluțiilor tehnologice*, modelarea acțiunilor concrete de utilizare prin construirea unor *tipologii*, și formularea unor *heuristici* bazate pe experiențele designerilor și utilizatorilor. Într-o primă instanță am analizat modelele implicite în tehnologii precum aplicațiile mobile de încurajare a renunțării la fumat sau jocurile serioase pentru educație. Într-o a doua instanță am studiat diversitatea stilurilor efective de interacțiune cu tehnologia pentru jocuri educaționale și alte platforme de învățare și generare de cunoaștere. În al treilea rând, am propus heuristici privind designul sistemelor gamificate, relevante și pentru crearea jocurilor serioase în educație și a arhitecturilor de medalii digitale.

O parte semnificativă dintre studiile pe care le-am publicat în domeniile securității, CSCL și HCI se bazează pe investigarea unor platforme și inițiative la dezvoltarea și coordonarea cărora am participat. Această convergență a cercetării și dezvoltării soluțiilor informatice ne-a permis o reflexivitate continuă privind propriile experiențe de designer și utilizator, precum și îmbunătățirea activităților noastre profesionale în comunitatea academică pe baza rezultatelor de cercetare.

A doua parte a tezei detaliază câteva direcții pentru activitatea viitoare de cercetare. În ceea ce privește studiul securității și confidențialității în Internet of Things, suntem interesați de optimizarea algoritmilor: deși prin eforturile realizate am arătat că serviciile bazate pe HVE ce folosesc localizarea pot fi implementate realist, rămân deschise zone de optimizare pentru soluții mai complexe. Urmărim să facem posibile solicitările referitoare la distanța dintre utilizator și un punct de interes din afara zonei sale geografice, scalarea către zone mai largi și numere mai mari de predicate, și armonizarea avantajelor tehnologiei Hidden Vector Encryption - HVE cu cele ale sistemelor bazate pe Private Information Retrieval - PIR, care nu necesită o terță parte în care utilizatorii să-și investească încrederea.

Suntem de asemenea interesați de studiul empiric al diversității orientărilor utilizatorilor către cyber-securitate, pentru a dezvolta metode eficiente de vizualizare și semnalizare online a informațiilor privind securitatea și confidențialitatea, pentru stimularea conștientizării corecte a riscurilor și a dezvoltării competențelor de prevenție și protecție prin comunicarea între egali, și pentru încurajarea practicilor de design care încorporează practici de securizare în Internet of Things.

O a treia direcție de interes se referă la cercetarea sistemelor mediate de calculator pentru generarea de cunoaștere. Suntem în special interesați de platformele colaborative prin care comunități mediate contribuie la soluționarea unor probleme specifice: feedback-ul utilizatorilor se cristalizează în *reputații* pentru activități online de comerț sau turism; comunitățile Q&A colectează *experiențe* care informează deciziile celor ce pun întrebări; sistemele wiki urmăresc generarea unor *documente multi-autorate* coerente; colective și comunități publică *expoziții* personale interactive. În astfel de situații online de interacțiune, urmărim să studiem felul în care tehnologia influențează accesul la perspective diferite asupra lumii; felul în care considerațiile relevante pentru decizii sunt modificate prin apelul la experiențele egalilor; felul în care înțelegerea și crearea sinelui este realizată prin noi tehnici de auto-monitorizare și management. Un proiect specific în această direcție se referă la 'Complex Accessible Remote LAboratories for Engineering Education and Applied Research' – CARLA, urmărind dezvoltarea competențelor inginerilor de diagnoză a situațiilor de eșec în cazul unor sisteme tehnologice complexe.