REZUMATUL TEZEI DE ABILITARE

elaborată de conf. univ.dr. SIMION EMIL

Teza prezintă realizările mele științifice, profesionale și academice ulterioare obținerii titlului de doctor, precum și direcțiile pe care le propun pentru dezvoltarea unei direcții proprii de cercetare, formarea unui grup de cercetare și desfășurarea activității de conducere de doctorat în domeniul Calculatoare, Tehnologia Informației și Ingineria Sistemelor.

Activitatea mea de cercetare este centrată pe generarea de secvențe binare aleatoare, validarea proprietăților lor statistice și analiza utilizării acestora în algoritmi și protocoale criptografice integrate în diverse soluții de securitate.

Securitatea unui sistem informatic nu este evaluată într-un singur punct, ci la mai multe niveluri, fiecare caracterizat prin propriile standarde și criterii. La nivelul algoritmilor și protocoalelor sunt esențiale robustețea construcțiilor și fundamentarea lor matematică. Modulele criptografice sunt reglementate de ISO/IEC 19790, echivalentul internațional al FIPS 140-3. Produsele și aplicațiile care integrează aceste module intră în domeniul ISO/IEC 15408 (Criteriile Comune) și al schemei europene EUCC. La nivelul sistemelor informatice și al organizațiilor în care acestea sunt utilizate se aplică familia de standarde ISO/IEC 27000, precum și cerințele Directivei NIS 2.

Lucrările prezentate în teză abordează mai multe dintre aceste niveluri și sunt unite de o experiență de douăzeci de ani în proiectarea algoritmilor criptografici și de zece ani în proiectarea soluțiilor de securitate. Această experiență îmi permite să pornesc de la un artefact sau o soluție inginerească, să îi analizez și să îi fundamentez riguros proprietățile, iar apoi să transform rezultatele obținute într-o decizie de proiectare. Această perspectivă interdisciplinară plasează teza în domeniul Calculatoare, Tehnologia Informației și Ingineria Sistemelor. Aparatul matematic este utilizat ca instrument pentru fundamentarea și validarea rezultatelor, în sprijinul obiectivelor inginerești și de securitate urmărite.

Astfel, în Capitolul 2 tratez proiectarea generatoarelor de numere aleatoare și pseudoaleatoare utilizate la producerea cheilor criptografice, inclusiv generatoarele cu adevărat aleatoare bazate pe oscilatoare în inel și elementele fundamentale de entropie pe care se sprijină implementarea și evaluarea acestora. Capitolul 3 este dedicat validării statistice a generatoarelor (pseudo)aleatoare, în special prin utilizarea bateriei NIST SP 800-22, și abordează corelația și (in)dependența testelor, estimarea analitică a erorii de ordinul al doilea și a puterii testelor, precum și ipotezele și limitele testării statistice în practica criptografică. Capitolul 4 prezintă rezultatele unor analize de securitate realizate în contexte și aplicații diverse, precum securitatea autovehiculelor, stocarea și mediile cloud, identificarea cheilor RSA publice slabe, teoria jocurilor, securitatea hardware și criptografia rezistentă la atacuri cuantice. Capitolul 5 descrie proiectele de cercetare în cadrul cărora s-a desfășurat această activitate, în special cele două granturi obținute prin competiție, în care am coordonat

echipa parteneră, respectiv am avut calitatea de director de proiect. În Capitolul 6 prezint activitatea mea didactică, activitatea de coordonare a cercetării și colaborările instituționale.

Capitolul 7 prezintă planul de dezvoltare a carierei academice și de cercetare, iar Capitolul 8 conține concluziile.