REZUMATUL TEZEI DE ABILITARE

Teza mea de abilitare prezintă activitatea profesională științifică și de cercetare pe care am desfășurat-o după susținerea tezei de doctorat la Universitatea Tehnică din Cluj-Napoca în data de 26 Mai 2009. În cadrul tezei de doctorat am elaborat metode pentru analiza formală a protocoalelor de securitate și am dezvoltat o metodă pentru compunerea acestor protocoale. În schimb, activitatea științifică pe care am desfășurat-o după obținerea titlului de Doctor în 2009, începând cu anul 2010 a avut ca obiective principale elaborarea de metode pentru protejarea infrastructurilor critice (en: Networked Critical Infrastructures – NCI).

Preocupările mele pentru acest domeniu au început odată cu câștigarea unui grant de cercetare de 3 ani (din Septembrie 2010 până în Septembrie 2013) acordat de Institutul pentru Protejarea și Securitatea Cetățenilor din cadrul Centrului de Cercetare Comun (Joint Research Centre) al Comisiei Europene, din Ispra, Italia.

Cercetările începute în cadrul acestui grant sunt continuate în momentul de față în cadrul unui proiect de 4 ani FP7 Marie Curie Career Integration Grant pe care l-am câștigat în 2014.

În consecință, teza mea de abilitare prezintă contribuțiile originale la îmbunătățirea securității și rezilienței NCI. Rezultatele pe care le-am obținut în domeniul tezei de abilitare sunt documentate în numeroase publicații științifice în cadrul unor reviste de specialitate (Communications of the ACM, IEEE Transactions on Emerging Topics in Computing, IEEE Systems Journal, International Journal of Critical Infrastructure Protection, Security and Communication Networks) și în cadrul unor conferințe și workshop-uri științifice (IEEE/IFIP Networking, ADHOC-NOW, IFIP CIP, EuroSec). Teza de abilitare este structurată după cum urmează.

Primul capitol realizează o introducere în domeniul protejării infrastructurilor critice și oferă o sinteză a tezei de abilitare, a principalelor contribuții și a lucrărilor în care au fost publicate rezultatele prezentate.

Capitolul 2 identifică cerințele pentru realizarea experimentelor de securitate cyber-fizice cu NCI: fidelitatea experimentelor, repetabilitatea experimentelor, acuratețea măsurătorilor și siguranța execuției experimentelor. Capitolul prezintă o nouă platformă de experimentare ce extinde Emulab cu simulatoare software pentru a satisface cerințele formulate. Metoda pe care am elaborat-o suportă experimente de securitate cu diverse infrastructuri precum cele chimice, rețele de electricitate și de transport.

Capitolul 3 prezintă o metodă pentru identificarea componentelor critice în NCI. Metoda elaborată se bazează pe metodologia de analiză a sistemelor dinamice. Aceasta măsoară impactul perturbațiilor, e.g., atac cibernetic, asupra ieșirii sistemelor și determină matricea de impact care cuantifică intervențiile realizate. Metoda elaborată a fost testată pe sisteme chimice și rețele de electricitate, fiind utilizată ca și intrare pentru metodele de proiectare ce urmează a fi detaliate în capitolele următoare.

Capitolul 4 descrie o metodă de optimizare liniară aplicată în proiectarea rețelelor NCI. Noutatea problemei constă în integrarea cerințelor de securitate definite în standardul ISA-62443.03.02, precum și în recomandările NIST Guide to Industrial Control Systems. Metoda pe care am elaborat-o permite proiectarea rețelelor pe baza unor criterii variate, precum securitatea comunicațiilor, arhitectura rețelei, lărgimea de bandă disponibilă, latența maximă permisă în comunicații, etc. Metoda a fost testată în diverse scenarii cu date provenite de la administratori de rețele și companii de energie.

Capitolul 5 prezintă o metodă de optimizare liniară pentru proiectarea rețelelor NCI reziliente la atacuri și perturbații. Metoda permite planificarea rețelei astfel încât aceasta să includă K căi alternative de rutare. Metoda a fost evaluată utilizând scenarii simulate.

Capitolul 6 prezintă o metodă de analiză non-intruzivă a serviciilor pentru identificarea vulnerabilităților software în cadrul NCI. Metoda extinde motorul de căutare Shodan cu algoritmi heuristici pentru reconstruirea identificatorilor de vulnerabilitate. Mai exact, am dezvoltat doi algoritmi pentru reconstruirea Common Platform Enumeration (CPE) și a Common Vulnerability Entry (CVE), pe care le-am integrat într-un nou instrument denumit ShoVAT (Shodan-based Vulnerability Assessment Tool). Metoda elaborată permite analiza istorică a vulnerabilităților software pentru înregistrări cuprinse în baza de date a Shodan.

Teza se încheie cu capitolul 7 în care sunt prezentate planul de dezvoltare a carierei profesionale, precum și direcțiile viitoare de cercetare.