Contribuții la asigurarea securității sistemelor informatice în mediul online
Autor: Gabriel-Marius PETRICĂ

Abstract: Importanța temei abordate de această teză de doctorat este subliniată de contextul actual, în care atacurile cibernetice devin tot mai variate și exploatează vulnerabilități hardware și software tot mai numeroase. În consecință, securitatea informațiilor și a sistemelor informatice a devenit o preocupare obligatorie în activitatea oricărei entități (individ sau organizație) care activează în domenii conexe conceptului TIC (Tehnologia Informației și a Comunicațiilor). Obiectivele principale ale lucrării au constat în realizarea unei analize a securității sistemelor informatice și a aplicațiilor Web și propunerea unor soluții pentru îmbunătățirea nivelului de securitate prin identificarea și clasificarea vulnerabilităților și a atacurilor cibernetice și adoptarea unor metode pentru limitarea efectelor acestora. Am aplicat, în cadrul unor studii de caz, trei metode de analiză a fiabilității / securității sistemelor: FMEA (Analiza modurilor de defectare și a efectelor), diagrama cauză-efect și arborii de defectare. Prin construirea unui arbore de atac-apărare și simularea mai multor scenarii am realizat o analiză cantitativă a gradului de realizabilitate a unui atac și am propus contramăsuri de apărare. Am identificat contexte potențial favorabile lansării unor atacuri malware prin intermediul poștei electronice sau al rețelelor wireless și am sugerat tehnici de micșorare a impactului acestor atacuri. Cercetările comparative privind tehnicile de „Apărare în profunzime” și „Apărare în lățime” au fost implementate prin dezvoltarea și securizarea unei platforme Web care a fost analizată din punctul de vedere al survivabilității (capacității de supraviețuire în cazul unor atacuri cibernetice) și al performanțelor, iar ulterior au fost aplicate soluții pentru îmbunătățirea acestor două aspecte.

Contributions to Security Assurance of Information Systems in Online Environment
Author: Gabriel-Marius PETRICĂ

Abstract: The importance of the subject approached by this PhD thesis is underlined by the current context in which cyber-attacks are becoming more and more variate and exploiting numerous hardware and software vulnerabilities. Consequently, the security of information and information systems has become a mandatory concern in the activity of any entity (individual or organization) operating in fields related to the ICT (Information and Communication Technology) concept. The main objectives of this work were to analyze the security of computer systems and Web applications and to propose solutions to improve security by identifying and classifying vulnerabilities and cyber-attacks and adopting methods to limit their effects. We have applied, in case studies, three systems reliability / security analysis methods: FMEA (Failure Mode and Effects Analysis), the cause-effect diagram and the Fault Trees. By building an Attack-Defense Tree and simulating multiple scenarios, we made a quantitative analysis of the feasibility of an attack and proposed defense countermeasures. We identified potentially favorable contexts for the launch of malware attacks via e-mail or wireless networks and we suggested techniques to reduce their impact. Comparative research on "Defense in depth" and "Defense in breadth" security techniques has been implemented by developing and securing a Web platform that has been analyzed from the point of view of survivability (ability to survive in the event of cyber-attacks) and performance, and then have been applied solutions to improve these two aspects.