UNIVERZITA KOMENSKÉHO FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

Abstract (SK):

Stromy útoku (attack trees) sú formálne modelové a analytické techniky, ktoré sa používajú na skúmanie potenciálnych hrozieb v rôznych druhoch systémov. V tejto práci pracujeme s stromami útoku ako s modelovou formuláciou na analýzu bezpečnostných výziev systémov s rôznymi scenármi útokov. Navrhli sme rôzne rozšírenia a varianty útočných stromov na analýzu zložitých modelov útočníkov. Navrhli sme tiež spôsoby, ako preložiť útočné stromy do časových automatov a potom použiť softvérový nástroj na vykonanie kontroly bezpečnostných vlastností. Okrem toho ich kombinujeme s vlastnosťou informačnej bezpečnosti s názvom opacity, aby sme zistili, či je možné pri neúplnej informácií odhaliť fázu útoku.

Medzi naše príspevky v tejto práci patrí zavedenie ochranných uzlov v útočných stromoch. To nám umožňuje modelovať možnú obranu proti akciám útočníkov na úrovni listov stromu. Navrhli sme tiež dynamické stromy útokov, ktoré možno použiť na modelovanie a analýzu systémov s dynamickými prostrediami hrozieb. Okrem rozšírenia množiny akcií, ktoré rozširujú základ útoku o časové trvanie, sme zaviedli aj časové obmedzenia, ktoré charakterizujú platnosť/úspešnosť útoku na množinu brán stromov. Potom sme ukázali, ako použiť koncept nepriehľadnosti na určenie, či útočník môže odhaliť niektoré skryté stavy systému. To sa vykonáva prekladom na kontrolu nepriehľadnosti aktuálneho stavu. Ďalej sme zaviedli reverzibilné útočné stromy ako variant útočných stromov, pri ktorých je možné prebiehajúci útok úplne alebo čiastočne vrátiť do pôvodného stavu stromov (systému).