INFORMAČNÝ SYSTÉM PRE ZISŤOVANIE ZRANITEĽNOSTI OBJEKTOV

Václavková Monika*,

ABSTRAKT

V príspevku je popisovaný návrh modelu informačného systému pre zisťovanie zraniteľnosti objektov a hodnotenie bezpečnostných systémov . Navrhovaný systém používa algoritmy pre hľadanie najkratšej cesty k chránenému záujmu s využitím pasívnej prelomovej odolnosti prvkov bezpečnostného systému. S ohľadom na zložitosť algoritmov prehľadávania ciest v grafoch je navrhnutá možnosť využitia paralelizmu v programovaní. Príspevok obsahuje popis jednotlivých modulov navrhovaného informačného systému. Databáza použiteľných prvkov bezpečnostného systému a ich parametrov uložená v informačnom systéme má širšie použitie. Popisovaný informačný systém má ďalšie možné rozšírenia . Existujú i ďalšie možnosti využitia popisovaného informačného systému v praxi bezpečnostného manažmentu.

Kľúčové slová: Zraniteľnosť, prvky bezpečnostného systému, pasívna prelomová odolnosť, hľadanie cesty v grafe, paralelné programovanie**.**

ABSTRACT

The concept of information system which is detected vulnerability of objects and assessment systems of security is described in the paper. The proposed system is used algorithms for searching the shortest path to protected interest with using passive break through endurance of items from security systems. With respects on complexities of scan graphs algorithms are proposed to use parallelism in programming. The paper is described modules specification of design informatics system. Database of usable items in project of security systems and its parameters which is saved in information system has a more possibilities. There are also next possibilities in expansion of design informatics system. Other possibilities of using described information system exist in practices of security management.

* Václavková Monika,Ing. Žilinská Univerzita v Žiline, Fakulta riadenia a informatiky, Katedra informatiky, Univerzitná 1, 010 26 Žilina, Monika.Vaclavkova@fri.uniza.sk

Key words: Vulnerability, elements of security system, passive break through endurance, searching path in graph, parallel programming.

1 ÚVOD

Podľa terminológie bezpečnostného manažmentu je zraniteľnosť definovaná ako tie časti objektu ochrany alebo tie prvky systému ochrany, ktoré nezabezpečujú požadovaný stupeň ochrany, sú slabým alebo ľahko prekonateľným prvkom v systéme ochrany[1]. V praxi bezpečnostného manažmentu je zisťovanie zraniteľnosti objektov, v ktorých sa nachádza chránený záujem jednou z dôležitých úloh . K rozhodujúcim kritériám pre spracovanie prehľadu zraniteľných miest chráneného objektu patrí aj trieda odolnosti pre použité mechanické zábranné prostriedky [1] a s tým súvisiaca ich úroveň prelomovej odolnosti, ktorá môže byť definovaná ako čas za ktorý je príslušný prvok prekonaný[2].

Pri posudzovaní a hodnotení existujúcich bezpečnostných systémov je potrebné, aby pre pozitívne hodnotenie systému bol čas, za ktorý páchateľ dosiahne chránený záujem väčší, dlhší , ako čas za ktorý bude páchateľ detekovaný, bude vyvolaná adekvátna reakcia, t.j. poplach a zásahová jednotka dorazí k objektu a realizuje príslušný zásah. Charakter niektorých chránených záujmov umožňuje do času páchateľovho pričítať i čas, za ktorý sa páchateľ snaží uniknúť, čiže opustiť objekt.

Dôležitý pre hodnotenie bezpečnostných systémov je fakt, že čas páchateľa je uvažovaný ten, ktorý je najkratší, t.j. uvažujeme s tým najhorším prípadom z hľadiska bezpečnostného systému. Ďalej je dôležité, že pre čas reakcie bezpečnostného systému platí to isté, t.j. uvažujeme s tým najhorším možným prípadom a vyberáme ten čas, ktorý je pre detekciu páchateľa a následný zásah najhorší a teda najdlhší.

V informačnom systéme, ktorého návrh ďalej popisujem sa bude pracovať takým spôsobom, aby sa v bezpečnostnom systéme vyhľadalo miesto, kde je zraniteľnosť najväčšia a to formou hľadania najkratšej cesty páchateľa k chránenému záujmu. Po nájdení tejto najkratšej cesty pre páchateľa, sa pre bezpečnostného manažéra ponúka možnosť analyzovať nájdenú cestu a mechanické zábranné prostriedky, ktoré sa na nej nachádzajú. V prípade potreby vylepšenia bezpečnostného systému je potrebné zvážiť triedy prelomovej odolnosti jednotlivých prvkov nachádzajúcich sa na nájdenej ceste.

Po analýze a prípadnej náhrade niektorého vybraného prvku kvalitnejším, t.j. s vyššou triedou odolnosti, je možné proces zopakovať a informačný systém použiť pre vyhľadanie novej najkratšej cesty v už upravenom bezpečnostnom systéme. Jednotlivých krokov opakovania procesu hľadania cesty môže byť niekoľko a ich počet môže závisieť od požadovaných parametrov pre účinnosť resp. kvalitu riešeného bezpečnostného systému.

2 POPIS NAVRHOVANÉHO INFORMAČNÉHO SYSTÉMU

2.1 REPREZENTÁCIA CHRÁNENÉHO OBJEKTU

Chránený objekt je možné v našom informačnom systéme reprezentovať prostredníctvom grafu. Uzlami grafu by sa mohli stať jednotlivé miestnosti, chodby

a ostatné priestory nachádzajúce sa v objekte. Pre každý z priestorov sa v systéme bude evidovať zoznam jednotlivých otvorových výplní, stien, podláh, stropov a podobne, ako i parametrov každého prvku zo zoznamu[2]. U otvorových výplní sa medzi parametrami budú evidovať: pozícia umiestnenia v priestore, rozmery a prelomová odolnosť daného prvku. U stien, podláh a stropov sa budú evidovať charakteristiky určujúce ich odolnosť (hrúbka, typ materiálu a podobne).

Hrany grafu je možné vytvoriť medzi jednotlivými priestormi nachádzajúcimi sa v objekte, ktoré spolu susedia a je možné sa medzi nimi fyzicky premiestňovať , resp. medzi jednotlivými prvkami v miestnosti. Každú hrana je možné ohodnotiť časom, za ktorý je možné sa premiestniť z uzla do uzla. Výpočet času závisí na určenej rýchlosti presunu medzi uzlami, pričom rýchlosť sa môže stať vstupným parametrom informačného systému. K uvedenému času by sa pripočítal čas potrebný na prekonanie mechanického zabezpečovacieho prvku, ktorý sa nachádza medzi oboma uzlami.

Problém hľadania najkratšej cesty pre páchateľa v zmysle času dosiahnutia chráneného záujmu, by sa potom mohol transformovať na problém hľadania najkratšej cesty v grafe. Problematika hľadania ciest v grafe je už dostatočne rozpracovaná a existuje niekoľko algoritmov, ktoré je možné využiť na tento účel v popisovanom informačnom systéme. Zložitosť algoritmov prehľadávajúcich graf a hľadajúcich všetky možné cesty, však s narastajúcim počtom uzlov prudko rastie. Jedným z vhodných algoritmov je známy Floydov algoritmus, ktorého zložitosť je možné odhadnúť pomocou vzťahu $O(n^3)$ [3]. Mnohé algoritmy na grafoch možno charakterizovať ako kombinatorické úlohy [4].

Na narastaní počtu uzlov závisí čas, za ktorý algoritmus prehľadá všetky cesty a nájde cestu najkratšiu. Ako z vzťahu vidno, závislosť je kubická , z čoho vyplýva, že s rastúcim počtom uzlov je časový nárast veľmi prudký. I keď dnešná výpočtová technika pokročila v oblasti parametrov hardwaru rýchlym tempom, pri danej zložitosti algoritmu je pre objekt s viacerými budovami a komplikovanou architektonickou skladbou, resp. viacpodlažnú budovu, časová odozva informačného systému neprijateľná pre podmienky v reálnom prostredí. Z tohto dôvodu je možné v popisovanom informačnom systéme využiť najmodernejšie smery skúmané a realizované v súčasnej informačnej vede, medzi ktoré patrí i paralelné spracovanie programov. Pre mnohé úlohy na grafoch existujú rozpracované paralelné algoritmy [5].

V paralelnom spracovaní programov sa využíva možnosť rozdeliť komplikovanú úlohu na jednotlivé čiastkové úlohy a tie sa potom paralelne riešia na viacerých procesoroch súčasne. Náš problém prehľadávania grafu vykazuje možnosť rozdeliť celkovú úlohu t.j. prehľadávanie celého grafu , na čiastkové úlohy, ktorými by mohlo byť prehľadávanie čiastkových podgrafov, resp. rozdelenie na hľadanie ciest vo viacerých budovách alebo na viacerých podlažiach paralelne. Takže aj pre architektonicky veľmi komplikované objekty by je možné čas realizácie algoritmu skrátiť na hodnoty prijateľné v reálnej prevádzke.

2.2 POPIS MODULOV INFORMAČNÉHO SYSTÉMU

2.2.1 KOMUNIKAČNÝ MODUL

Úlohou komunikačného modulu informačného systému je interakcia s používateľom. Prostredníctvom tohto modulu si používateľ zadáva vstupné parametre do systému. Komunikačný modul je ďalej zodpovedný za každú ďalšiu interakciu s používateľom, ako napríklad zmenu parametrov, opakovanie výpočtov, zmena prvkov práve riešeného bezpečnostného systému a podobne. Nevyhnutnými vstupmi do informačného systému sú charakteristiky objektu ako napríklad architektonické členenie objektu, povaha perimetra, plášťov jednotlivých budov, charakteristiky striech, stropov, podláh, otvorových výplní a rozmiestnenie jednotlivých prvkov bezpečnostného systému. Okrem toho je úlohou komunikačného modulu realizovať spojenie s databázovým modulom a prostredníctvom neho ukladať, meniť a načítavať údaje z databázy. V neposlednom rade je úlohou komunikačného modulu interpretácia vypočítaných výsledkov a teda reprezentácia výstupných dát pre používateľa.

2.2.2 MODUL PRE VÝPOČTY

Úlohou modulu pre výpočty je realizácia všetkých potrebných výpočtov. Modul musí realizovať transformáciu pôdorysu objektu s existujúcimi, prípadne navrhovanými prvkami práve riešeného bezpečnostného systému do reprezentácie prostredníctvom grafu. Následne je potrebné vyriešiť pomocou zvoleného algoritmu pre prehľadávanie grafu nájdenie najkratšej cesty k chránenému záujmu pre páchateľa. V prípade riešenia uvedeného problému s veľkým počtom uzlov a hrán v grafe modul pre výpočty môže realizovať algoritmus na viacerých procesoroch paralelne. Modul pre výpočty taktiež interaguje s komunikačným modulom, ako i s databázovým modulom.

2.2.3 DATABÁZOVÝ MODUL

Databázový modul má za úlohu prácu s databázou. Skladá sa z dvoch častí. Prvou časťou databázového modulu je samotná databáza, v ktorej sú uložené dáta. Informácie uložené v databáze môžu mať v prípade popisovaného informačného systému dvojaký charakter. Jeden typ dát by mali byť jednotlivé bezpečnostné prvky, ktoré je možné použiť do projektu bezpečnostného systému. Bezpečnostné prvky by mali mať v databáze uložené svoje charakteristiky, medzi ktorými nesmú chýbať popis prvku a jeho trieda pasívnej prelomovej odolnosti.

Ďalší typ dát by mali byť jednotlivé projekty bezpečnostných systémov, ktoré už boli informačným systémom spracovávané. Ide o dáta, týkajúce sa skladby objektov, v ktorých sa chránený záujem nachádza, spolu s navrhovanými prvkami, ktoré boli do bezpečnostného systému umiestnené v poslednej interakcii s používateľom. Uložené projekty je možné kedykoľvek z databázy vybrať a projekt bezpečnostného systému opätovne upravovať, ak to používateľ požaduje. Možnosť úprav už existujúceho projektu uloženého v databáze, v sebe zahrňuje potenciál dynamicky sledovať meniace sa podmienky a jednotlivé riziká, ktoré na chránený záujem majú vplyv a prispôsobovať im projekt bezpečnostného systému.

Druhou časťou databázového modulu by mal byť systém riadenia bázy dát, ktorý pozostáva z programového vybavenia zabezpečujúce všetku prácu s databázou.

V súčasnosti sú v praxi najčastejšie používanými databázovými systémami systémy s relačnými databázami. Relačné databázové systémy umožňujú prísne kontroly prístupu do databázy, kontroly dát ukladaných do databázy, vzťahov medzi dátami v databáze , ako i prístupové práva na jednotlivé operácie v databáze. Sú teda dostatočne bezpečnými systémami pre prácu s databázou, v ktorej sa nachádzajú dáta s citlivým charakterom informácie.

Nakoľko v súčasnosti na Slovensku neexistuje databáza jednotlivých bezpečnostných prvkov , ktoré by mohli byť súčasťou bezpečnostného systému, bolo by potrebné databázu uvedených prvkov vytvoriť. Popisovaný systém si vyžaduje uloženie jednotlivých prvkov s ich požadovanými charakteristikami v databáze, nakoľko sú nevyhnutne potrebné pre prácu systému. Avšak uvedená databáza by po naplnení mohla slúžiť i na iné účely v praxi manažmentu bezpečnostných rizík.

Vytvorenie uvedenej databázy si vyžaduje roztriediť uvažované prvky bezpečnostných systémov do druhov, prípadne kategórií a zhromaždiť informácie o charakteristikách jednotlivých prvkov. Po následnom uložení do databázy budú informácie prístupné jednak popisovanému systému, ale i použiteľné na prípadné ďalšie účely.

2.3 MOŽNÉ ROZŠÍRENIA POPISOVANÉHO INFORMAČNÉHO SYSTÉMU

Doposiaľ popisovaný informačný systém mal za úlohu zaoberať sa zraniteľnosťou bezpečnostných systémov, prípadne hodnotením bezpečnostných systémov. Je však možné informačný systém rozšíriť o ďalšiu funkcionalitu.

V informatických vedách je jednou z moderných expandujúcich oblastí umelá inteligencia. Umelá inteligencia zahŕňa celý rad možných aplikácií svojich teoretických znalostí. Jedným zo spôsobov využitia umelej inteligencie, ktorá je často používaná v praxi, sú expertné systémy[6].

Expertné systémy sú charakteristické tým, že v sebe nesú uložené znalosti expertov z danej problematiky a uvedené znalosti využívajú pri svojej práci. V našom prípade by sa jednalo o znalosti expertov z oblasti bezpečnostného manažmentu.

V expertných systémoch sa často využívajú takzvané heuristiky[6], t.j. informácie prípadne znalosti, ktoré často nie sú vedecky podložené, ale expert používa tieto znalosti vo svojej práci a ich využitie mu umožňuje skvalitnenie jeho práce. Ide o znalosti empirického charakteru, ktoré expert získal počas svojej praxe. V našom systéme by heuristické znalosti mohli byť využité pri nahrádzaní jednotlivých prvkov bezpečnostného systému.

Modul pre výpočty vyhľadá používateľovi najkratšiu cestu v grafe, teda najkratšiu cestu pre páchateľa k chránenému záujmu. Na tejto ceste však môže byť viacero mechanických zábranných prvkov a bezpečnostný manažér – začiatočník nemá ešte také skúsenosti, ktorý prvok by bolo najvhodnejšie nahradiť a aký prvok z palety vhodných ako náhradu zvoliť. Ak by systém mal uložené znalosti skúseného experta v uvedenej problematike, mohol by sám ponúknuť úpravy prvkov na nájdenej najkratšej ceste. Stal by sa tak pomocníkom pri projektovaní nového bezpečnostného systému, prípadne pri vylepšovaní existujúceho bezpečnostného systému.

3 ZÁVER

Popisovaný bezpečnostný systém sa dá použiť na viaceré účely v praxi bezpečnostného manažmentu. Umožňuje sa v ňom centralizovane viesť evidenciu a hierarchiu typov jednotlivých používaných prvkov bezpečnostných systémov. Ďalej by sa v ňom umožňuje prácovať so zraniteľnosťou u existujúcich projektov bezpečnostných systémov. Informačný systém by bolo možné využiť aj pri hodnotení bezpečnostných systémov. Po uvedených rozšíreniach by bolo možné použiť popisovaný systém ako podporný prostriedok pri projektovaní bezpečnostných systémov pre začínajúcich bezpečnostných manažérov. Okrem toho by mohol informačný systém slúžiť ako prostriedok pri výučbe danej problematiky.

Možnosti využitia popisovaného informačného systému v praxi, ale i teórii bezpečnostného manažmentu sú široké. Je samozrejme možné ďalej systém rozširovať prípadným napojením na ďalšie softwarové produkty. Z uvedeného vyplýva, že popisované informačné technológie by mohli slúžiť v bezpečnostnom manažmente ako podporné prostriedky a skvalitňovať, či uľahčovať prácu bezpečnostných manažérov.

LITERATÚRA

[1] MIKOLAJ, J., HOFREITER, L., MACH, V., MIHÓK, J., SELINGER, P.: Terminológia bezpečnostného manažmentu. FŠI ŽU. Žilina: Multiprint s.r.o. 2004. 191 s. ISBN 80-969148-1-2.

[2] REITŠPÍS, J., MESÁROŠ, M., BARTLOVÁ, I., ČAHOJOVÁ, Ľ., HOFREITER, Ľ., SELINGER, P., Manažérstvo bezpečnostných rizík. EDIS 2004. 289 s. ISBN 78-80-8070-823-8.

[3] VARŠA, P.: Príspevok k zložitosti distribuovaných paralelných algoritmov, dizertačná práca. FRI ŽU. Žilina, 2003. 94 s.

[4] GRONDŽÁK, K., MARTINCOVÁ, P.: Parallel solving of large combinatorial problems . In: Proceedings of the 18th international conference on systems for automation of engineering and research (SAER-2004) : 24-26 September 2004, St. Konstantin resort, Varna, Bulgaria. - Sofia: Technical University, 2004. - ISBN 954-438-428-6. - PP. 51-54.

[5] GRONDŽÁK, K., MARTINCOVÁ, P. AND CHOCHLÍK, M.:Performance analysis of parallel algorithm for backtracking. In: GCCP 2008 : 4th International workshop on Grid computing for complex problems : October 27 - 29, 2008, Bratislava, Slovakia : proceedings. - Bratislava: Institute of Informatics SAS, 2008. - ISBN 978-80-969202-9-7. - PP. 38-45.

[6] KELEMEN, J., LIDAY, M.: Expertné systémy pre prax. SOFA 1996. 201 s. ISBN 80-85752-32-8.

článok recenzoval:
doc. Ing. Zdeněk Dvořák, PhD