

Meno:

Mgr. Štefan Pero



Ukončený stupeň štúdia:

Druhý, magister

Názov záverečnej práce:

Distribučované dolovanie dát

Abstrakt:

Diplomová práca sa zaoberá problematikou distribuovaných výpočtov v oblasti dolovania dát. V práci sa analyzujú rôzne distribuované systémy, ich výhody a nevýhody použitia. Hlavným cieľom je navrhnúť distribuovaný systém a vytvoriť model transformácie klasického algoritmu na distribuovaný algoritmus. V práci sa konkrétne rozoberá framework Hadoop a programovací model MapReduce. V ďalšom kroku sa implementujú distribuované algoritmy k-means klastrovanie a matrix factorization. Práca obsahuje aj výsledky testov a porovnaní časových nárokov na výpočty daných problémov.

Meno:

Mgr. Pavol Sokol



Ukončený stupeň štúdia:

Druhý, magister

Názov záverečnej práce:

Kritériá hodnotenia bezpečnosti informačných systémov

Abstrakt:

Práca sa zaoberá problematikou hodnotenia kritérií bezpečnosti informačných systémov. Využitím najrozšírenejších kritérií hodnotenia bezpečnosti informačných systémov – Common Criteria (ISO/EIC 15408) sa podrobnejšie venuje profilu ochrany pre autentifikáciu do lokálnej počítačovej siete (hodnotený systém). Podľa dostupných noriem a materiálov načrtáva pre túto autentifikáciu bezpečnostný problém a v nadväznosti na neho stanovuje bezpečnostné ciele pre hodnotený systém a pre operačné prostredie, v ktorom bude tento systém umiestnený. Práca analyzuje aj legislatívny rámec hodnotenia bezpečnosti informačných systémov v platnej legislatíve SR. Podstatná časť práce je venovaná profilu ochrany a jeho najdôležitejšej časti - funkčným požiadavkám hodnoteného systému. Medzi tieto požiadavky zaraďujeme funkčné bezpečnostné požiadavky a požiadavky na bezpečnostné záruky. Práca určuje zoznam funkčných bezpečnostných požiadaviek, ktoré sú nevyhnutné preto, aby sme mohli systém označiť ako bezpečný a uvádza zoznam požiadaviek na bezpečnostné záruky, ktorými sa určujú postupy pri tvorbe, implementácii a používaní takéhoto informačného systému. Súčasťou časti práce je aj praktická implementácia systému pre autentifikáciu do lokálnej počítačovej siete zohľadňujúc niektoré bezpečnostné ciele a funkčné požiadavky zadané v profile ochrany. Zvoleným protokolom pre implementáciu hodnoteného systému je protokol 802.1x s použitím FreeRADIUS servera.

Práca podáva postup pri inštalácii a konfigurácii tejto implementácie s upozornením na jej bezpečnostné aspekty.

Meno:

Bc. Marek Šafárik



Ukončený stupeň štúdia:

Prvý, bakalár

Názov záverečnej práce:

Vizualizácia funkčného AES kryptografického systému

Abstrakt:

V dnešnej dobe, keď sa na internete uchováva stále viac osobných údajov a väčšina platieb prebieha cez internet je stále dôležitejšie šifrovanie a ochrana dát. Taktiež výkon osobných počítačov zatiaľ nezastaviteľne rastie, vďaka čomu sa stávajú útoky hrubou silou, prípadne iné útoky stále dostupnejšie. A aj to je jeden z dôvodov, prečo sa začala hľadať náhrada za šifrovací systém DES, ktorý už nebol dostatočne odolný voči útokom. Ako vhodná náhrada sa ukázala šifra Rijndael, z ktorej bol neskôr odvodený šifrovací štandard AES. A práve tomuto štandardu sa táto práca venuje. Práca vysvetľuje rozdiely medzi symetrickou a asymetrickou kryptografiou a bližšie popisuje AES kryptografický systém. Hlavným cieľom tejto bakalárskej práce je vytvoriť funkčnú aplikáciu v Jave, ktorá bude vizualizovať beh AES algoritmu.