INFORMATIKA

Problémy implementácie kryptografických primitív do sieťových protokolov.
školiteľ: doc. RNDr. Jozef Jirásek, PhD.
forma štúdia: denná alebo externá
Anotácia: Dnešné zabezpečené sieťové protokoly Internetu používajú súčasne niekoľko kryptografických primitív v rôznych kombináciách a v rôznych režimoch. Aj keď jednotlivé primitíva sú podrobené mnohým bezpečnostným analýzam, ich súčasné používanie môže viesť k ďalším neočakávaným zraniteľnostiam. Práca bude analyzovať možnosti paralelných útokov na primitíva, používané kryptografické funkcie a spôsoby ich použitia so zámerom dokázať dosiahnuteľnosť konkrétnych bezpečnostných cieľov, prípadne navrhnúť ochranu pred zistenými zraniteľnosťami.

Plasticita a pozornosť v priestorovom počúvaní.
školiteľ: doc. Ing. Norbert Kopčo, PhD.
forma štúdia: denná
Anotácia: V každodennom živote sú ľudia vystavení rôznym súčasne pôsobiacim stimulom v komplexnom a neustále sa meniacom prostredí. V snahe korektne extrahovať relevantné informácie ľudia adaptovali spracovávanie vnemov tak, aby odrážalo špecifiká aktuálnej scény, a z predošlých skúseností sa naučili zlepšovať použité stratégie vnímania. Cieľom projektu je na základe vykonanej série behaviorálnych experimentov, štúdií zobrazenia mozgu a s využitím výpočtového modelovania študovať ako pozornosť a mechanizmus implicitného a explicitného učenia vplýva na zvládnutie spracovania reči, lokalizácie zvuku a učenia sa nových fonetických kategórii v komplexných zvukových prostrediach.

Krosmodálne interakcie v priestorovom sluchu.
školiteľ: doc. Ing. Norbert Kopčo, PhD.,
forma štúdia: denná
Anotácia: Naše videnie ovplyvňuje ako vnímame priestor sluchom. Bruchomluvecký efekt a afterefekt sú fenoménmi, ktoré ilustrujú krátkodobú plasticitu v priestorovom sluchu vyvolanú vizuálnymi signálmi. Vizuálny pozornostný cuing tiež ovplyvňuje sluchové vnímanie z hľadiska lokalizácie zvukov aj priestorového benefitu pri spracovaní reči. Tento projekt bude skúmať efekt vizuálnej informácie na priestorové sluchové vnímanie s využitím behaviorálnych experimentov, neuroimagingových štúdií a výpočtového modelovania.

Brain-training hry a priestorové počutie.
školiteľ: doc. Ing. Norbert Kopčo, PhD.
forma štúdia: denná
Anotácia: Dostupné možnosti zlepšenia počutia u ľudí s klinicky zdravým sluchom sú obmedzené, a žiadna z nich nie je akceptovaná ani rozšírená tak ako načúvacie strojčeky a kochleárne implantáty. Cieľom tohto projektu je prispieť k vývoju nových procedúr pre rehabilitáciu sluchového postihu vývojom brain-training hier založených na najnovších poznatkoch sluchovej neurovedy a výskume v rámci EU Horizon 2020 grantu ALT. Vývoj sluchovej brain-training hry bude v spolupráci s University of California, Riverside Brain Game Center a Oregon Health & Science University. Hlavným cieľom je vývoj a testovanie rehabilitatívnych techník, ktoré majú zlepšiť sluchové funkcie u ľudí so zhoršeným výkonom v testoch sluchových deficitov tréningom rôznych aspektov sluchového vnímania.

Formálna konceptová analýza.
školiteľ: prof. RNDr. Stanislav Krajči, PhD.,
forma štúdia: denná alebo externá
Anotácia: Formálna konceptová analýza je data-minigová metóda na obdĺžnikovej tabuľke, ktorej každý riadok zodpovedá nejakému objektu, každý stĺpec nejakému jeho potenciálnemu atribútu a každé políčko obsahuje informáciu o tom, či (prípadne v akej miere) má príslušný objekty príslušný atribút. Jeden z cieľov tejto metódy je nájsť takzvané koncepty, čo sú v istom zmysle stabilné dvojice podmnožín objektov a atribútov. FCA možno považovať za peknú aplikáciu algebraického pojmu Galoisovej konexie. Pôvodná verzia vychádza z klasického diela Gantera a Willeho a popisuje prípad binárnych dát. Vzniká však prirodzená otázka, čo sa stane, ak údaje v tabuľke nebudú binárne...

Grafovo-algoritmické aspekty komunikačných sietí.
školiteľ: prof. RNDr. Gabriel Semanišin, PhD.
forma štúdia: denná forma
Anotácia: V súvislosti s rozvojom Internetu vecí je potrebné riešiť viaceré aspekty komunikácie jednotlivých súčastí počítačových a senzorových sietí. Tieto siete sa dajú modelovať pomocou konceptov z oblasti teórie grafov. Následne je možné formulovať a riešiť algoritmické problémy, ktoré súvisia s efektívnym vytváraním takýchto sietí, prenosom údajov a ich zabezpečením. Táto problematika je veľmi živá a v poslednom období vzniklo pomerne veľké množstvo prác tak teoretického ako aj aplikačného významu.

Analýza údajov zo senzorov s využitím metód strojového učenia.
školiteľ: prof. RNDr. Gabriel Semanišin, PhD.
konzultant RNDr. Ľubomír Antoni, PhD.
forma štúdia: denná
Anotácia: Riešenia dátovej analýzy sa využívajú v rôznych oblastiach technických, prírodných, humanitných a ekonomických vied. Strojové učenie je podoblasťou umelej inteligencie, ktorá sa zaoberá metódami a algoritmami učenia sa stroja na základe vstupných údajov v definovanom priestore riešení. Cieľom dizertačnej práce je navrhnúť a aplikovať algoritmy a metódy učenia sa pomocou stroja v prípadových štúdiách analýzy údajov zo senzorov a porovnať úspešnosť navrhnutého riešenia s inými dostupnými štúdiami.

Analýza digitálnych stôp pomocou metód strojového učenia.
školiteľ: prof. RNDr. Gabriel Semanišin, PhD.
konzultant RNDr. JUDr. Pavol Sokol, PhD.
forma štúdia: denná
Anotácia: Digitálna forenzná analýza sa stala nevyhnutnou súčasťou reakcie na počítačové bezpečnostné incidenty ako aj súčasťou vyšetrovania kybernetickej kriminality. Dôležitú fázu forenzného vyšetrovania predstavuje samotná analýza digitálnych stôp. V rámci tejto fázy je potrebné extrahovať forenzné artefakty, určiť ich relevantnosť, hodnotu pre daný prípad, ako aj vzťahy medzi nimi. Účelom tejto fázy je potvrdenie, resp. vyvrátenie forenzných hypotéz stanovených v prvotných fázach forenzného vyšetrovania. Cieľom tejto práce je analyzovať možnosti používania metód strojového učenia pri analýze digitálnych stôp vzhľadom na komplexnosť, množstvo a heterogénnosť forenzných artefaktov. Súčasne je cieľom

navrhnúť spôsob výberu pre prípad relevantných forenzných artefaktov, nájdenia vzťahu medzi nimi ako aj overenia samotnej forenznej hypotézy.

Forenzná analýza internetu vecí.
školiteľ: prof. RNDr. Gabriel Semanišin, PhD.
konzultant RNDr. JUDr. Pavol Sokol, PhD.
forma štúdia: denná alebo externá
Anotácia: Internet vecí (IoT) sa stáva neoddeliteľnou súčasťou bežného života. To so sebou súčasne prináša aj významný nárast bezpečnostných hrozieb a bezpečnostných incidentov. Dôležitým aspektom pri vyšetrovaní počítačových bezpečnostných incidentoch je adekvátne forenzné vyšetrovanie. V rámci tohto vyšetrovania je možno identifikovať viacero problémov, ktoré sú spojené s heterogenitou dostupných komponentov vytvárajúcich IoT. Cieľom práce je analyzovať možnosti použitia metód strojového učenia pri zaisťovaní, extrakcii a analýze digitálnych stôp z týchto zariadení ako aj navrhnúť automatizovaný spôsob extrakcie a analýzy forenzných artefaktov z IoT komponentov.

Modelovanie a algoritmizácia konštrukcie hladkých kriviek.
školiteľ: doc. RNDr. Csaba Török, CSc.
forma štúdia: denná
Anotácia: Nedávno sme navrhli nový prístup k riešeniu trojdiagonálnych sústav ne rovnomernej sieti uzlov. Jedným z cieľov doktorandskej práce je preskúmanie vplyvu daného prístupu na nerovnomerné siete a inverziu trojdiagonálnych matíc. Klasické kubické splajny triedy C^2 sú zadané implicitne. Nám sa podarilo ich vyjadrenie v explicitnom tvare, čo umožňuje návrh lineárneho modelu aproximácie a odhad koeficientov splajnu. Druhým cieľom DP je analýza vlastností MNŠ odhadu koeficientov a ich porovnanie s B-splajnami. Tretím cieľom je hľadanie kritéria optimálneho zastavenia pri on-line aproximácii vzhľadom na prognózovanie vo vhodnej metrike.

Shannonova vzorkovacia veta a reálne problémy.
školiteľ: doc. RNDr. Csaba Török, CSc.
forma štúdia: denná
Anotácia: Vzorkovacia veta, založená na funkcii sinc, poskytuje dostatočné podmienky, ktoré zaručujú, aby nekonečné diskrétne postupnosti zachytili všetky informácie zo spojitého signálu a tak umožnili jeho úplnú rekonštrukciu. Vďaka nej pre prax je možné vypracovať rôzne geometrické, fyzikálne či numerické modely. Pozorované signály, postupnosti reálnych záznamov či simulovaných a vypočítaných údajov sú však konečné a prax ukázala, že na ich popis, interpoláciu, aproximáciu, analýzu uvažovať iba sinc funkcie, predovšetkým v prípade rovnomerných uzlov, je nedostatočné. Otázkou je, ako navrhovať reálne modely, aby ich aplikácia bola presná a efektívna.

Útoky na metódy strojového učenia v oblasti kybernetickej bezpečnosti.
doc. RNDr. Csaba Török, CSc.,
konzultant: RNDr. JUDr. Pavol Sokol, PhD.
forma štúdia: denná
Anotácia: Metódy strojového učenia zohrávajú v rámci reakcie na bezpečnostné incidenty dôležitú úlohu. K detekcii bezpečnostných incidentov, resp. útokov tieto metódy vytvárajú z tréningových údajov modely normálneho správania a detegujú

incidenty, resp. útoky ako odchýlky od tohto modelu. Tento proces nabáda útočníkov, aby manipulovali s tréningovými údajmi takým spôsobom, aby naučený model nedokázal odhaliť ich následné útoky. Okrem fázy učenia sa, sú bezpečnostné systémy využívajúce metódy strojového učenia náchylné na rôzne útoky aj vo fáze samotného rozhodovania. Útočník pomocou špeciálne vybraných vstupov obíde naučené správanie sa detekčného systému. Cieľom tejto práce je analyzovať používané metódy strojového učenia v oblasti kybernetickej bezpečnosti vzhľadom na ich odolnosť voči vyššie uvedeným útokom. Súčasne je cieľom navrhnúť spôsob testovania metód strojového učenia vzhľadom na možnosť ich zneužitia zo strany útočníka a spôsob ochrany týchto metód voči rôznym typom útokov.

Interkontextové štruktúry a zachovanie informácie.
školiteľ: doc. RNDr. Ondrej Krídlo, PhD.
forma štúdia: denná
Anotácia: Formálna konceptová analýza (FCA) poskytuje nástroje na extrakciu implicitných znalostí z ľubovoľných tabuľkových dát. Výzvou tejto dizertačnej práce by mal byť výskum v prostredí prepájania viacerých tabuliek pri zachovaní vnútorných štrukturálnych a znalostných vlastností vstupných dát. K tomuto už od svojich počiatkov FCA disponuje teoretickými nástrojmi, ktoré ale neberú v úvahu istú sémantickú stránku tohto problému. Najnovšie výsledky pochádzajúce z nášho ústavu ale ukazujú cestu, ktorou je bezpečné sa vydať. Je to stále len začiatok. Výstupom tejto dizertačnej práce by malo byť pokračovanie či už po teoretickej či algoritmickej stránke vyžadujúce aj značnú dávku experimentovania s rôznymi reálnymi dátami.