INFORMATIKA / INFORMATICS

Problémy implementácie kryptografických primitív do sieťových protokolov. Problems of cryptographic primitives implementations in network protocols

školiteľ/ supervisor: doc. RNDr. Jozef Jirásek, PhD. (jozef.jirasek@upjs.sk)
forma štúdia / study from: denná alebo externá / full time or external

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.

Annotation: Nowadays, secure internet protocols are using several cryptographic primitives at the same time in different combinations and in different modes. Even though the individual primitives are subject to many security analyzes, their current use can lead to further unexpected vulnerabilities. The work will analyze the possibilities of parallel attacks on the primitives, used cryptographic functions and the methods of their use with the intention of proving the feasibility of specific safety objectives, or propose protection against identified vulnerabilities.

Plasticita a pozornosť v priestorovom počúvaní. Plasticity and attention in spatial hearing

školiteľ/ supervisor: doc. Ing. Norbert Kopčo, PhD. (norbert.kopco@upjs.sk)
forma štúdia / study from: denná / full time

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.

Annotation: In everyday situations, humans are exposed to multiple concurrent stimuli in complex, continuously changing environments. To correctly extract relevant information, they adapt their processing to reflect the specifics of the current scene, and they learn from previous experience to improve the perceptual strategies used. The current project proposes to perform a series of behavioral experiments, brain imaging studies, and computational modeling to study how attention and mechanisms of implicit and explicit learning are used to cope with complex listening environments for speech processing, sound localization, and learning of new phonetic categories.

Krosmodálne interakcie v priestorovom sluchu.
Cross-modal interactions and spatial auditory processing

školiteľ/ supervisor: doc. Ing. Norbert Kopčo, PhD. (norbert.kopco@upjs.sk)
forma štúdia / study from: denná / full time

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.

Annotation: Vision influences how we perceive space by hearing. Ventriloquism effect and after-effect are phenomena illustrating short-term plasticity in spatial hearing induced by visual signals. Visual attentional cuing also influences spatial auditory processing both in terms of sound localization and spatial benefit in speech perception. The current project will examine the effect of visual information on spatial auditory perception by performing behavioral experiments, neuroimaging studies, and computational modeling.

Formálna konceptová analýza
Formal concept analysis

školiteľ/ supervisor: prof. RNDr. Stanislav Krajči, PhD., (stanislav.krajci@upjs.sk)
forma štúdia / study from: denná alebo externá / full time or external

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...

Annotation: Formal concept analysis is a data-mining method applied to a rectangular matrix of data in which each row corresponds to some object, each column corresponds to some possible attribute, and the matrix field value denotes a membership of the column attribute for row object. One of the goals of this method is to find so-called concepts, which are stable (in some sense) pairs of subsets of objects and attributes. The method can be considered a nice application of the algebraic notion of a Galois connection. It has been described in detail by Ganter and Wille, in particular for the so-called crisp case with binary matrix data. A natural question that arises is what happens if the matrix data are non-binary...

Grafovo-algoritmické aspekty komunikačných sietí.
Graph theoretical and algorithmic aspects of communication networks

školiteľ/ supervisor: prof. RNDr. Gabriel Semanišin, PhD. (gabriel.semanisin@upjs.sk)
forma štúdia / study from: denná / full time

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.

Annotation: The development of Internet of Things requires solutions for various aspects of a communication in computer and sensor networks. These networks can be modelled by graph-theoretical concepts. Such models provide bases for a formulation and solution of algorithmic problems that are related to network creation, data transfer and securing. These topics are studied very extensively and relatively big number of recent papers with significant theoretical and practical impact was published recently.

Analýza údajov zo senzorov s využitím metód strojového učenia
Analysis of sensor data using machine learning methods

školiteľ/ supervisor: prof. RNDr. Gabriel Semanišin, PhD. (gabriel.semanisin@upjs.sk)
konzultant / consultant: RNDr. Ľubomír Antoni, PhD.
forma štúdia / study from: denná / full time

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.

Annotation: Data analysis solutions are applied in various areas of technical, natural, human and economic sciences. Machine learning is a sub-area of artificial intelligence that deals with machine learning methods and algorithms based on input data in a defined solution space. The aim of the dissertation thesis is to design and application of algorithms and methods of machine learning in case studies of sensor data analysis and to compare the performance of the proposed solution with other available studies.

Analýza digitálnych stôp pomocou metód strojového učenia
Analysis of digital evidence using machine learning methods

školiteľ/ supervisor: prof. RNDr. Gabriel Semanišin, PhD. (gabriel.semanisin@upjs.sk)
konzultant / consultant: RNDr. JUDr. Pavol Sokol, PhD.
forma štúdia / study from: denná / full time

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.

Annotation: Digital forensic analysis has become an essential part of responding to cybersecurity incidents as well as part of cybercrime investigation. An important phase of forensic investigation is the analysis of digital evidence itself. Within this phase, it is necessary to extract forensic artefacts, determine their relevance, value for the case, as well as relationships between them. The purpose of this phase is to confirm, resp. reject the forensic hypotheses established in the early stages of the forensic investigation. The aim of this work is to analyze the possibilities of using machine learning methods in the analysis of digital tracks with respect to the complexity, volume, and heterogeneity of forensic artefacts. At the same time, the aim is to propose a method of selection for the case of relevant forensic artefacts, to find a relationship between them as well as to verify the forensic hypothesis itself.

Forenzná analýza internetu vecí
Forensic analysis of the internet of things

školiteľ/ supervisor: prof. RNDr. Gabriel Semanišin, PhD. (gabriel.semanisin@upjs.sk)
konzultant / consultant: RNDr. JUDr. Pavol Sokol, PhD.
forma štúdia / study from: denná alebo externá / full time or external

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.

Annotation: The Internet of Things (IoT) is becoming an integral part of everyday life. Also, it brings a significant increase in security threats and security incidents. An important aspect of the investigation of computer security incidents is an adequate forensic investigation. Within this investigation, several problems can be identified that are related to the heterogeneity of the available IoT-producing components. The aim of the work is to analyze the possibilities of using machine learning methods in securing, extraction and analysis of

digital tracks from these devices as well as to design an automated method of extraction and analysis of forensic artefacts from IoT components.

Modelovanie a algoritmizácia konštrukcie hladkých kriviek
Modeling and algorithms for construction of smooth curves

školiteľ/ supervisor: doc. RNDr. Csaba Török, CSc. (csaba.torok@upjs.sk)
forma štúdia / study from: denná / full time

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.

Annotation: Recently we proposed a new approach to solving the tridiagonal systems on a uniform grid of nodes. One of the goals of the thesis is to investigate the effect of the given approach on the nonuniform grid and the inversion of tridiagonal matrices. Classic cubic splines of class C^2 are implicit. We succeeded to express them in an explicit form that enables a design of a linear model for approximation and estimate of spline coefficients. The second goal is to analyze the properties of LS estimate of coefficients and their comparison with B-splines. The third goal is finding of criterion of optimal stopping in on-line approximation according to prediction in an appropriate metric.

Shannonova vzorkovacia veta a reálne problémy.
Shannon's sampling theorem and real problems

školiteľ/ supervisor: doc. RNDr. Csaba Török, CSc. (csaba.torok@upjs.sk)
forma štúdia / study from: denná / full time

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.

Annotation: The sinc function based sampling theorem provides sufficient conditions to guarantee that infinite discrete sequences capture all the information from the continuous signal and thus enables the full reconstruction of the original one. Thanks to it, it is possible to develop various geometric, physical or numerical models for practice. However, observed signals, sequences of real records or simulated and calculated data are final, and practice has shown that for their effective description, interpolation, approximation or analysis it is insufficient to consider only sinc functions, especially in the case of uniform nodes. The

question is how to design the models so that they can be used effectively in applications and give the most accurate results.

Útoky na metódy strojového učenia v oblasti kybernetickej bezpečnosti
Attacks on machine learning methods in the field of cybersecurity

školiteľ/ supervisor: doc. RNDr. Csaba Török, CSc. (csaba.torok@upjs.sk)
konzultant / consultant: RNDr. JUDr. Pavol Sokol, PhD.
forma štúdia / study from: denná / full time

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.

Annotation: Machine learning methods play an essential role in responding to security incidents. To detect security incidents, respectively security attacks, these methods make training data models of normal behaviour and detect incidents, respectively attacks as deviations from these models. This process encourages the attackers to manipulate training data in such a way that the learned model cannot detect their subsequent attacks. In addition to the learning phase, security systems using machine learning methods are also vulnerable to various attacks during the decision-making phase. Using specially selected inputs, the attacker bypasses the learned behaviour of the detection system. This work aims to analyze used machine learning methods in the field of cybersecurity concerning their resistance to the above attacks. At the same time, the aim is to propose a method of testing machine learning methods with regard to the possibility of their misuse by the attacker and how to protect these methods against various types of attacks.

Interkontextové štruktúry a zachovanie informácie.
Intercontext structures and information preserving

školiteľ / supervisor: doc. RNDr. Ondrej Krídlo, PhD. (ondrej.kridlo@upjs.sk)
forma štúdia / study from: denná / full time

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.

Annotation: Formal Concept Analysis (FCA) provides tools for extracting implicit knowledge from any tabular data. The challenge of this dissertation should be research in the environment of interconnecting multiple tables while maintaining the internal structural and knowledge properties of the input data. The FCA has had theoretical tools for this since its inception, but it does not take into account the semantic side of this problem. But the latest results coming from our institute pave the way which one can find out. It's still just the beginning. The output of this dissertation should be a continuation, whether from a theoretical or algorithmic point of view, they also needed a considerable amount of experimentation with various real data.