Informačné vzdelávanie

**Určenie typu a vhodnosti informačných zdrojov**

**Meno**: Emma Macháčová

**Názov seminárnej práce:** Bezpečnosť - šifrovanie

**Dátum:** 24.10.2019

**Adversarial Data Mining: Big Data Meets Cyber Security**

Názov seminárnej práce: Bezpečnosť - šifrovanie

Dátum: 24.10.2019

|  |
| --- |
| **Názov informačného zdroja a odkaz na informačný zdroj :** |
| ACM Digital Library  <https://dl.acm.org/citation.cfm?id=2976753> |
| **Typ zdroja (článok z časopisu/príspevok zo zborníka/kapitola z monografie/monografia) :** |
| Príspevok zo zborníka |
| **Čo som zistila, naučila sa z informačného zdroja?** |
| Prehľad o najnovšiom vývoji v získavaní kontradiktórnych údajov, techniky a aplikácie získavania kontradiktórnych údajov v aplikáciách kybernetickej bezpečnosti a ako využiť existujúce nástroje na správu veľkých dát na vytváranie algoritmov získavania údajov pre kybernetickú bezpečnosť. |
| **Ako získané informácie môžem použiť vo svojej práci?** |
| Môžem nimi priblížit problematiku kyberbezpečnosti v súčastnosti |

**Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems**

Názov seminárnej práce: Bezpečnosť - šifrovanie

Dátum: 24.10.2019

|  |
| --- |
| **Názov informačného zdroja a odkaz na informačný zdroj :** |
| IEEE  <https://ieeexplore.ieee.org/document/8232537> |
| **Typ zdroja (článok z časopisu/príspevok zo zborníka/kapitola z monografie/monografia) :** |
| Článok z časopisu |
| **Čo som zistila, naučila sa z informačného zdroja?** |
| Tento dokument definuje model ohrozenia bezpečnosti / zabezpečenia pre systémy CPS a IoT a zisťuje nové techniky, ktoré zlepšujú bezpečnosť a zabezpečenie systémov CPS a IoT. |
| **Ako získané informácie môžem použiť vo svojej práci?** |
| Popis kyber-fyzických systémov (CPSs), internetu vecí (IoT) v súvislosti s počítačovou bezpečnosťou a výpočtovým modelovaním |

**Cyber security concept for Internet of Everything (IoE)**

Názov seminárnej práce: Bezpečnosť - šifrovanie

Dátum: 24.10.2019

|  |
| --- |
| **Názov informačného zdroja a odkaz na informačný zdroj :** |
| IEEE  <https://ieeexplore.ieee.org/document/7997540> |
| **Typ zdroja (článok z časopisu/príspevok zo zborníka/kapitola z monografie/monografia) :** |
| Príspevok zo zborníka |
| **Čo som zistila, naučila sa z informačného zdroja?** |
| Popis šifrovacieho mechanizmu, vrstvený šifrovací mechanizmus, ako funguje hash chain, hlavné zásady pri určovaní opatrení na zabezpečenie informačnej bezpečnosti, čo je to metodológia Cybex |
| **Ako získané informácie môžem použiť vo svojej práci?** |
| Rozšírenie informácií témy bezečnosť a Internet of Everything |

**Secure data-sharing using distributed environmental matching keys**

Názov seminárnej práce: Bezpečnosť - šifrovanie

Dátum: 24.10.2019

|  |
| --- |
| **Názov informačného zdroja a odkaz na informačný zdroj :** |
| ScienceDirect  <https://www.sciencedirect.com/science/article/pii/S1574119217300470> |
| **Typ zdroja (článok z časopisu/príspevok zo zborníka/kapitola z monografie/monografia) :** |
| Článok z časopisu |
| **Čo som zistila, naučila sa z informačného zdroja?** |
| “Aby sme poskytli bezpečnú a efektívnu metódu zdieľania údajov v cloudovom prostredí, v tomto článku sme vytvorili protokol šifrovania bezpečných cloudových dát, ktorý je pomenovaný kľúčom zdieľania údajov zdieľaného kľúčom environmentálnej zhody (skratka EMaDS). EMaDS šifruje zdieľané údaje pomocou jedného šifrovacieho kľúča, ktorý kombinuje niekoľko kľúčov zodpovedajúcich prostrediu odvodených z hesla oprávneného používateľa a hardvérovej / softvérovej konfigurácie dôveryhodného zariadenia.” |
| **Ako získané informácie môžem použiť vo svojej práci?** |
| Vysvetlenie zmyslu šifrovania, reálne využitie, aké problémy môžu nastať, riziká a opatrenia |

**Advanced Data Encryption**

Názov seminárnej práce: Bezpečnosť - šifrovanie

Dátum: 24.10.2019

|  |
| --- |
| **Názov informačného zdroja a odkaz na informačný zdroj :** |
| ScienceDirect  <https://www.sciencedirect.com/science/article/pii/B978012416681300015X> |
| **Typ zdroja (článok z časopisu/príspevok zo zborníka/kapitola z monografie/monografia) :** |
| Kapitola z monografie |
| **Čo som zistila, naučila sa z informačného zdroja?** |
| Kvantová kryptografia je založená na rámci kvantovej fyziky a je určená na riešenie problému distribúcie kľúčov, ktorá je podstatnou súčasťou kryptografie, ktorá umožňuje zabezpečenie údajov. Kľúč umožňuje, aby boli dáta kódované tak, že na dekódovanie údajov by bolo potrebné poznať kľúč, ktorý sa použil na kódovanie údajov. |
| **Ako získané informácie môžem použiť vo svojej práci?** |
| Rozšírenie informácií o funkcii kľúčov |

**Data Encryption and Authetication Using Public Key Approach**

Názov seminárnej práce: Bezpečnosť - šifrovanie

Dátum: 24.10.2019

|  |
| --- |
| **Názov informačného zdroja a odkaz na informačný zdroj :** |
| ScienceDirect  <https://www.sciencedirect.com/science/article/pii/S1877050915006705> |
| **Typ zdroja (článok z časopisu/príspevok zo zborníka/kapitola z monografie/monografia) :** |
| Článok z časopisu |
| **Čo som zistila, naučila sa z informačného zdroja?** |
| Ako môže buť Euler Totientova teoréma využitá na vytvorenie množiny čísel, ktoré šifrujú tok údajov |
| **Ako získané informácie môžem použiť vo svojej práci?** |
| Prídavok k téme šifrovanie |

**A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System**

Názov seminárnej práce: Bezpečnosť - šifrovanie

Dátum: 24.10.2019

|  |
| --- |
| **Názov informačného zdroja a odkaz na informačný zdroj :** |
| IEEE  <https://ieeexplore.ieee.org/document/7307787> |
| **Typ zdroja (článok z časopisu/príspevok zo zborníka/kapitola z monografie/monografia) :** |
| Príspevok zo zborníka |
| **Čo som zistila, naučila sa z informačného zdroja?** |
| Technika hybridného šifrovania je nové kryptografické paradigma a môže sa uplatniť na internet vecí. |
| **Ako získané informácie môžem použiť vo svojej práci?** |
| Informácie ku kryptovacím algorytmom |