ALVERAD
SECURITY TESTING LABORATORY

I. ALVERAD-BÁNKI

Nemzetközi Kiberbiztonsági Konferencia

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS
BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Budapest, 2023. október 25.

I. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencia

I. Alverad-Bánki International Cybersecurity Conference

Konferenciakötet

Book of abstracts

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

BÁNKI DONÁT GÉPÉSZ ÉS
BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

BÁNKI DONÁT FACULTY OF MECHANICAL
AND SAFETY ENGINEERING

Kiadó / Publisher: Óbudai Egyetem

Felelős kiadó / Editor-in-Chief: Prof. Dr. Rajnai Zoltán

Szerkesztette / Edited by: Dr. Répás József

Műszaki szerkesztő / Technical Editor: Horváth Richárd

ISBN 978-963-449-344-0

online elérhető / online available at: https://www.alverad.hu

Köszöntő

Az Alverad Technology Focus Kft. és az Óbudai Egyetem Bánki Kara a Kiberbiztonsági hónap keretében 2023. október 25-én első alkalommal rendezte meg hibrid formában nemzetközi tudományos konferenciáját.

A konferencia célja volt, hogy a legújabb hazai és nemzetközi kutatási eredményeket a szakértő közönség számára elérhetővé tegyük, továbbá lehetőséget biztosítsunk a fiatal kutatók, a PhD hallgatók számára a publikációs gyakorlat megszerzésére, továbbá, hogy a társegyetemek oktatói és hallgatói, valamint kollégáink tudományos kapcsolatai is elmélyüljenek.

Az előadók névsora, a helyszín, a kísérőprogramok, valamint a szervezők elismertsége garantálta a hiánypótló és hasznos rendezvényt. Az előadások témagazdagsága és sokszínűsége hűen tükrözi napjaink kiberbiztonsági kihívásokban gazdag időszakát, illetve a legújabb kutatási trendeket és irányokat.

Ezúton szeretnénk köszönetet mondani elsősorban az előadóknak, és mindazoknak, akik részt vettek az esemény megvalósításában, támogatták, valamint ösztönzésükkel és segítségükkel nagyban hozzájárultak e kiadvány megjelenéséhez.

Budapest, 2023. 12. 15.

Hinkel Attila	Prof. Dr. Rajnai Zoltán
Ügyvezető	Dékán

Greetings

Alverad Technology Focus Ltd. and the Bánki Faculty of Óbuda University successfully organized their first international scientific conference in a hybrid format on October 25, 2023, within the framework of European Cybersecurity Month.

The conference aimed to make the latest domestic and international research results accessible to the expert audience and provide an opportunity for young researchers and PhD students to gain experience in publication practices. Furthermore, the goal was to deepen the scientific relations between lecturers and students of partner universities.

The lineup of speakers, the location, the accompanying programs, and the recognition of the organizers ensured a unique and valuable event. The richness and diversity of the presentations faithfully reflected today's cybersecurity challenges, the latest research trends and directions.

We would like to express our gratitude Hereby, we would like to thank primarily the speakers and all those who participated, supported, and with their encouragement and help greatly contributed to the publication of this publication.

We would like to express our gratitude primarily to the speakers and all those who participated in the realization of the event, supported it and greatly contributed towards making this publication possible with their encouragement and assistance.

Budapest, December 15, 2023.

Attila Hinkel

CEO

Prof. Dr. Zoltán Rajnai

Dean

Szervezőbizottság / Organizing Committee

Tiszteletbeli elnök / Honorary chair

Hinkel Attila (Alverad Technology Focus Kft.)

Általános elnök / General chair

Prof. Dr. Rajnai Zoltán (Óbudai Egyetem – ÓE BGK)

Általános társelnök / General co-chair

Dr. Számadó Róza (Óbudai Egyetem – ÓE BGK)

Tudományos bizottság elnöke / Scientific Committee chair

Prof. Dr. Berek Lajos (Óbudai Egyetem – ÓE BGK)

Tudományos bizottság / Scientific Committee

Dr. Kovács László, tudományos rektorhelyettes (Nemzeti Közszolgálati Egyetem / National University of Public Service – NKE)

Dr. Berek Tamás (Nemzeti Közszolgálati Egyetem / National University of Public Service – NKE)

Dr. Wersényi György (Széchenyi István Egyetem / Széchenyi István University – SZE)

Dr. Huszti Andrea (Debreceni Egyetem / Debrecen University – DE)

Dr. Hidvégi Timót (Széchenyi István Egyetem / Széchenyi István University – SZE)

Dr. Répás József (Nemzeti Közszolgálati Egyetem / National University of Public – NKE)

Tartalomjegyzék / Contents

Kiberbiztonság - I. szekció – IoT és OT

Cybersecurity - session I.– IoT and OT

Kiberbiztonság - I. szekció – IoT és OT

ADATCSOMAGANALIZÁLÁS MESTERSÉGES INTELLIGENCIÁVAL PYTHON NYELVEN

DOBRÁDY Zoltán, HIDVÉGI Timót

Napjainkban az ipari adatátviteli – kommunikációs - hálózatok jelentős fejlődéseken estek át, amit a hozzá szorosan köthető biztonsági intézkedések nem minden esetben követtek. Az egyes ipari rendszerek perifériáinak száma, illetve a közöttük zajló hálózati forgalom is nagyságrendekkel megnövekedett. Ezeket az adatokat egy hiba, anomália, illetve egy kibertámadás esetén elemezni kell. Napjainkban ezt utólag, szöveges szűrőkkel, célszoftverekkel, illetve legvégső esetben manuálisan viszik végbe. A fenti problémára sokkal kézenfekvőbb megoldás lenne, ha ezek az elemzések kvázi valós időben, még az adott periférián belül történnének meg. Az elemzések eredményeit felhasználva, mesterséges intelligencia segítségével egy modell alkotható. Ezt a modellt felhasználva már akár lehetőség nyílhat egy adott anomália prediktálására. A Python nyelv azért került kiválasztásra, mert számtalan elemzési metodikával rendelkezik, illetve a már tanított AI modellek könnyen exportálhatóak.

Kulcsszavak:

Csomagelemzés, mesterséges intelligencia, OT biztonság, Python, valós idejű analízis

Cybersecurity - session I.– IoT and OT

DATA PACKET ANALYSIS WITH ARTIFICIAL INTELLIGENCE WRITTEN IN PYTHON

Zoltán DOBRÁDY, Timót HIDVÉGI

Nowadays, industrial data transmission on communication networks has undergone significant developments, where related security measures were not always able to keep up. The number of peripheral devices within distinct industrial units and the flow of information across the network has also grown significantly. In the event of a mishap, anomaly, or online intrusion, this information must be examined. Currently, this is accomplished retrospectively, employing text filters, target software or, as a last resort, by hand. A more plausible resolution to the aforementioned issue would be for these analyses to occur in quasi-real time, still within the peripheral region. Thanks to artificial intelligence, a model can be created using the results of the analyses. By utilizing this model, it may be feasible to predict a specific anomaly. The python language was chosen because it has a lot of different ways to analyze data and AI models that have already been trained can be easily exported.

Keywords:
Packet analysis, AI, OT security, Python, real time analysis

Kiberbiztonság - I. szekció – IoT és OT

FELÜGYELET NÉLKÜLI ANOMÁLIAFELISMERÉS MESTERSÉGES INTELLIGENCIA SEGÍTSÉGÉVEL CAN BUSZ ADATCSOMAGOKBAN

DOBRÁDY Zoltán

Napjainkban a kommunikáció egyik legmeghatározóbb csatornája a CAN busz. Ez nem csak az autóiparban, de más iparágakban is népszerű, így a forgalomirányító jelzőlámpák kommunikációjához is előszeretettel használják. Több kereszteződés lámpáit egyetlenegy központ is képes vezérelni, ahova az adatok hosszú kábelszakaszokon érkeznek. Nem csak a kábelen indukálódott zajokat, de a kibertámadásokat is figyelembe kell venni. Akár egy kábel manipulálása esetén a teljes kereszteződés jelzőlámpáinak az adatfolyamára rálátásunk lehet. Belátható, hogy a keletkezett anomáliákat elemezni kell. Mesterséges intelligenciát használva lehetőség nyílik az adatfolyam valós idejű analizálására, ami a hagyományos módszerekkel megoldhatatlan lenne. Ebben a kutatásban többféle, nem felügyelt anomália detekciós metódust fogok elemezni, illetve összehasonlítani mesterséges intelligenciával.

Kulcsszavak:

Anomália keresés, mesterséges intelligencia, OT biztonság, CAN bus, valós idejű analízis

Cybersecurity - session I.– IoT and OT

UNSUPERVISED ANOMALY DETECTION IN CAN BUS DATA PACKETS USING ARTIFICIAL INTELLIGENCE

Zoltán DOBRÁDY

The CAN bus is one of the most important ways to communicate in today's world. It is not only used in the automotive industry, but also in other sectors, such as the communication of traffic control signal lights. A single central unit is capable of controlling the lights at multiple intersections, where data is transmitted over long cable spans. Cyberattacks hold equal significance to the noise generated on the cable and require consideration. One could gain access to the entire data stream of the intersections traffic lights by cable manipulation. Clearly, the anomalies that arise must be analysed. Using artificial intelligence, it is possible to analyse the data stream in real-time, which would be impossible with traditional methods. This investigation will examine and compare various unsupervised approaches for detecting anomalies by using AI.

Keywords:
Anomaly Detection, AI, OT security, CAN bus, real time analysis

Kiberbiztonság - I. szekció – IoT és OT

IPARI HÁLÓZATOK TITKOSÍTÁSI LEHETŐSÉGEI

HIDVÉGI Timót

Az Ipar 4.0 megjelenése felkészületlenül érte a különböző gyárakat és termelőüzemeket. Ma az az elvárás, hogy minden mérési eredményt és adatot a felhőben tároljanak. Különböző ajánlások, eszközök és architektúrák jelentek meg, hogy ezt az elvárást minél kényelmesebbé tegyék. Az alapvető probléma azonban megmaradt, nevezetesen az, hogy az ipari eszközök (PLC-k, beavatkozók, szenzorok, robotok stb.) különböző titkosítatlan protokollok segítségével kommunikálnak egymással. Az ipari eszközök kommunikációjára általában a Modbus protokollt használják (minden OT eszközben ez megtalálható, nem gyártóspecifikus), amely nagyon kényelmes, de nem titkosított, azaz a hálózati forgalomban láthatóak az érzékeny adatok (pl. jelszó, mérési eredmények stb.). A gyártósorok egyik fő jellemzője, hogy ritkán állítják le, és a különböző frissítések megvalósításához menetrendet kell készíteni. Ezért az évek óta elkészült és működő ipari rendszerek üzemeltetőitől sajnos nem várható el az, hogy átálljanak a titkosított protokollok használatára. Ezeket a protokollokat a PLC-gyártók általában még nem készítették el. Cikkünk egy olyan tesztkörnyezetet, illetve protokolljavaslatot ír le, amely kényelmesen megvalósítható a meglévő ipari hálózatokban.

Kulcsszavak:
Ipari hálózat, titkosítatlan protokoll, OSI modell, saját készítésű protokoll, purdue modell

Cybersecurity - session I.– IoT and OT

ENCRYPTION POSSIBILITIES OF INDUSTRIAL NETWORKS

Timót HIDVÉGI

The appearance of Industry 4.0 was unprepared for various factories and production plants. Today, the expectation is that all measurement results and data will be stored in the cloud. Various recommendations , tools and architectures have emerged to make this expectation as convenient as possible. However, the basic problem remained, namely that industrial devices (PLCs, actuators, robots, etc.) communicate with each other using unencrypted protocols. For industrial devices communication, Modbus is usually used, which is very convenient to use but unencrypted, i.e., sensitive data (e.g., password, measurement results, etc.) are visible in network traffic. One of the main features of production lines is that they are rarely shut down, and a timetable must be drawn up for the implementation of the various upgrades. Therefore, industrial systems that have been completed and operating for years are unfortunately not expected to switch to using encrypted protocols. These protocols are generally not yet prepared by PLC manufacturers. Our article describes a test environment or protocol proposal that can be conveniently implemented in existing industrial networks.

Keywords:
Operational technology, uncrypted protocols, OSI model, purdue model, own protocol

Kiberbiztonság - II. szekció – Drónok

Cybersecurity - session II.– Drones

Kiberbiztonság - II. szekció – Drónok

DRÓNOK HÁLÓZATÁHOZ KAPCSOLÓDÓ REGISZTRÁCIÓS PROTOKOLL ÉS BIZTONSÁGI KÉRDÉSEI

MOLNÁR Botond, OLÁH Norbert

Az elmúlt években a pilóta nélküli repülőgépek (UAV-k) használata szignifikánsan növekedett számos területen, például a mezőgazdaságban vagy a logisztikában. Azonban a gyors terjedés mellett számos biztonsági kérdés merül fel. Az általunk javasolt pehelysúlyú (lightweight) regisztrációs protokoll fontos újítása a PUF (Physical Unclonable Function) és a blokklánc technológia használata. A drónok hálózatához kapcsolódó támadások közül kiemelt figyelmet fordítottunk a fizikai támadásokra, melyek a legegyszerűbben kivitelezhetőek és nagyon effektívek. Emellett a hálózati szinten megvizsgáltuk a gyakran előforduló elosztott túlterheléses támadást (DDoS), amelyre egy megoldás lehet a neurális hálók alkalmazása. Ennek segítségével el lehet dönteni, hogy az adott frekvencia használható-e még kommunikációra. Abban az esetben, ha nem, akkor az összes eszköznek frekvenciát kell váltani. Végezetül az adatvédelmi kérdések (privacy) drónok hálózatához kapcsolódó szempontjait értékeljük ki.

Kulcsszavak:

Drón, drónok internete, PUF, blokklánc, kriptográfiai protokoll

Cybersecurity - session II.– Drones

INTERNET OF DRONES RELATED REGISTRATION PROTOCOL AND SECURITY CONCERNS

Botond MOLNÁR, Norbert OLÁH

In recent years, the use of unmanned aerial vehicles (UAVs) has increased significantly in many fields, such as agriculture and logistics. However, this rapid expansion is accompanied by a number of safety issues. An important innovation of our proposed lightweight registration protocol is the use of PUF (Physical Unclonable Function) and blockchain technology. Among the attacks related to the drone network, we have focused on physical attacks, which are the easiest to implement and very effective. In addition, at the network level, we examined the frequently occurring distributed denial of service (DDoS) attack, for which one solution could be the use of neural networks. This can be used to decide whether a given frequency can still be used for communication. In case it is not, all devices will have to change frequencies. Finally, the privacy aspects of the drone network will be evaluated.

Keywords:
Drone, Internet of Drones, PUF, blockchain, cryptographic protocol

Kiberbiztonság - II. szekció – Drónok

DRÓN FORENSICS MÓDSZERTAN ALKALMAZÁSÁNAK VIZSGÁLATA MAGAS AUTOMATIZÁLTSÁGÚ CIVIL ÉS KATONAI JÁRMŰVEK SZAKÉRTŐI VIZSGÁLATÁBAN

RÉPÁS József

A modern polgári és katonai járművek közlekedési baleseteinek vagy a hozzájuk kapcsolódó egyéb bűncselekmények utólagos szakértői vizsgálatának egyik célja annak megállapítása, hogy milyen esemény, mikor, hol és milyen körülmények között történt. A járművek automatizálási szintjének növekedésével széles körben terjednek el az ún. csatlakoztatott megoldások (pl. drón-jármű együttműködés). A járművekben és a hozzájuk csatlakoztatott drónokban pontos idővonalat és hiteles bizonyítékokat lehet biztosítani a vizsgált eseményekről. A drónok szakértői vizsgálata, a drónokban tárolt és a kommunikációs csatornákon továbbított adatok feltárásával, feldolgozásával, értelmezésével, elemzésével foglalkozik, melynek egyes vizsgálati lépései a járművek vizsgálata esetén is alkalmazhatók lehetnek. Jelen tanulmány célja, hogy megvizsgálja a Digital forensics egyik területét, a Drone forensics-et, annak megállapítására, hogy annak mely lépései vagy eljárásai alkalmazhatók a magasan automatizált és egyre inkább autonóm járművek (pl. katonai járművek) szakértői vizsgálata során.

Kulcsszavak:

Drón, szakértői vizsgálatok, autonóm járművek, módszertan

Cybersecurity - session II.– Drones

EXAMINATION OF THE APPLICATION OF DRONE FORENSICS METHODOLOGY OF THE HIGHLY AUTOMATED CIVIL AND MILITARY VEHICLES

József RÉPÁS

One of the aims of digital forensics investigations into modern civil and military vehicles traffic accidents or other crimes is to establish what kind of incident occurred, when, where, and under what circumstances. As vehicles' automation level increases, connected solutions become more widespread (e.g., drone-vehicle cooperation), and an accurate timeline of events and credible evidence can be provided in vehicles and connected drones. The forensic examination of drones deals with the exploration, processing, interpretation, and analysis of data stored in drones and sent through the established communication channel, some of the examination steps of which may be applicable in the case of vehicle examination. This study aims to examine one of the areas of digital forensics, Drone forensics, to determine which of its steps or procedures can be applied in the expert examination of highly automated and increasingly autonomous vehicles (e.g. military vehicles).

Keywords:
Drone, digital forensics, autonomous vehicles, methodology

Kiberbiztonság - II. szekció – Drónok

PILÓTA NÉLKÜLI LÉGIJÁRMŰBŐL KINYERHETŐ DIGITÁLIS NYOMOK FELHASZNÁLÁSI LEHETŐSÉGEI, KORLÁTAI

RÉPÁS József, RIPSZÁM Dóra

A drónok, vagy más néven pilóta nélküli légi járművek elterjedésével a használati célok is széles spektrumot fednek le. Ideértve a nagy területek fényképezését és videofelvételek készítését, környezeti felmérések elvégzését, járművek kiterjesztett érzékelését, valamint katonai műveletek végrehajtását is. A technológiai fejlesztések következtében a drónok ma már számos kiegészítő technológiát tartalmaznak, beleértve a nagy teljesítményű kamerákat, hőszkennereket, sőt akár még katonai fegyvereket is. A pilóta nélküli légijárművekből kinyerhető digitális nyomok fontos szerepet játszhatnak egyéb eljárások mellett a büntetőeljárásban is. Ezek sikeres felhasználásának érdekében a nyomozó hatóságok szakértőket és szaktanácsadókat, illetve szervezeten belül elemző értékelőket vehetnek igénybe. A nyomok, a bizonyítás körében hasznosak lehetnek, azonban alkalmazásuknak vannak bizonyos törvényi korlátai.

Kulcsszavak:

Drón, szakértői vizsgálatok, digitális nyomok, módszertan

Cybersecurity - session II.– Drones

USAGE POSSIBILITIES AND LIMITATIONS OF DIGITAL EVIDENCE THAT CAN BE ACQUIRED FROM UNMANNED AERIAL VEHICLE

József RÉPÁS, Dóra RIPSZÁM

With the spread of drones, also known as unmanned aerial vehicles, the purposes of use also cover a wide spectrum. This includes taking photographs and video recordings of large areas, carrying out environmental surveys, vehicle extended detection, as well as carrying out military operations. As a result of technological advances, drones now include many additional technologies, including high-powered cameras, thermal scanners, and even military weapons. The digital evidence that can be acquired from unmanned aerial vehicles can play an important role in criminal proceedings, among other procedures. In order to use them successfully, investigative authorities can use forensics experts and consultants. Traces can be useful in the field of evidence, but their application has certain legal limitations.

Keywords:
Drone, digital forensics, digital evidence, methodology

Kiberbiztonság - III. szekció – Intelligens környezetek

Cybersecurity - session III.– Intelligent environments

Kiberbiztonság - III. szekció – Intelligens környezetek

ZERO TRUST ARCHITEKTÚRA (ZTA) KIALAKÍTÁSA INTELLIGENS ÉPÜLETEKBEN

SÁNDOR Barnabás, RAJNAI Zoltán

A mai digitális környezetben az összekapcsolt dolgok internetének (IoT) eszközeivel felszerelt intelligens épületek a fejlett kiberfenyegetések középpontjává váltak. A hagyományos, kerület-alapú biztonsági modellek gyakran nem képesek kezelni az ilyen intelligens infrastruktúrákban rejlő bonyolult sebezhetőségeket. Ez a kutatás a Zero Trust architektúrák (Zero Trust Architectures, ZTA), mint az intelligens épületrendszerek védelmének paradigmaváltását szolgáló megoldások elfogadásával és megvalósításával foglalkozik. A hagyományos modellekkel ellentétben, amelyek implicit bizalomra épülnek, a ZTA azon az elven alapul, hogy alapértelmezés szerint egyetlen belső vagy külső egységben sem szabad alapból megbízni. Átfogó elemzéssel ez a tanulmány megvilágítja, hogy a ZTA miként javíthatja a hozzáférés-ellenőrzést, minimalizálhatja a bennfentes fenyegetéseket, és granuláris biztonsági intézkedéseket biztosíthat, biztosítva, hogy minden eszköz, felhasználó és hálózati áramlás hitelesített és engedélyezett legyen. A folyamatos felügyelet és a legkisebb jogosultság elveinek integrálásával a ZTA az intelligens épületek egyedi kihívásaira szabott, robusztus védelmi mechanizmust kínál. Az eredmények kiemelik a ZTA-ban rejlő lehetőségeket az intelligens épületrendszerek kiberbiztonsági protokolljainak forradalmasításában, megnyitva az utat egy biztonságosabb és ellenállóbb digitális épített környezet felé.

Kulcsszavak:
Zero Trust Architektúra, Intelligens épületrendszerek. IoT biztonság, Hozzáférés-ellenőrzés, Kiberbiztonsági protokollok

Cybersecurity - session III.– Intelligent environments

ZERO TRUST ARCHITECTURES (ZTA) FOR SMART BUILDING SYSTEMS

Barnabás SÁNDOR, Zoltán RAJNAI

In today's digital environment, intelligent buildings equipped with Internet of Things (IoT) devices have become the focus of advanced cyber threats. Traditional perimeter-based security models often need help to address the complex vulnerabilities inherent in such intelligent infrastructures. This research focuses on adopting and implementing Zero Trust Architectures (ZTA) as a paradigmshifting solution for protecting intelligent building systems. Unlike traditional models, which are based on implicit trust, ZTA is based on the principle that no internal or external entity should be trusted by default. Through a comprehensive analysis, this paper sheds light on how ZTA can improve access control, minimize insider threats, and provide granular security measures, ensuring that all devices, users, and network flows are authenticated and authorized. By integrating the principles of continuous monitoring and least privilege, ZTA offers a robust security mechanism tailored to the unique challenges of intelligent buildings. The results highlight the potential of ZTA to revolutionize cybersecurity protocols for intelligent building systems, paving the way toward a more secure and resilient digital built environment.

Keywords:
Zero Trust Architecture, Smart Building Systems. IoT Security, Access Control, Cyber Security Protocols

Kiberbiztonság - III. szekció – Intelligens környezetek

A BOTNETEK LEHETSÉGES FELHASZNÁLÁSA A MALWAREK DETEKTÁLÁSÁBAN

SÁNTA Máté Imre, OLÁH Norbert

Manapság a kiberbűnözés hatalmas méreteket öltött, súlyos károkat okozva mind a felhasználóknak, mind a vállalatoknak, ahol a támadók egyik fontos eszköze a rosszindulatú szoftverek (malwarek) használata. Így a malwarek detektálása és semlegesítése a biztonság egyik központi témaköre, mivel igazán átfogó és mindenre kiterjedő megoldással nem rendelkezünk és a terület folyamatosan fejlődik és változik.

Az általunk javasolt megoldás egy malwareket detektáló botnet, amely képes megfelelő kommunikációra és adatküldésre. A botnet egy Yara szkennert használ, amely képes a Yara szabályainkat megfelelően kezelni, vagy akár kategorizálni azokat. A felhasználóbarát platform megvalósításának érdekében készítettünk egy webes felhasználói felületet, ahol ellenőrizhetjük az elkapott karanténba kerülő malwareket. Emellett elkészítésre kerültek a szabályok, szabálykészletek, amelyek a leggyakoribb, illetve a jelenlegi „legnépszerűbb” malwereken alapulnak.

Kulcsszavak:

Biztonság, malware, botnet, Yara, vírusírtó

Cybersecurity - session III.– Intelligent environments

THE POTENTIAL USE OF BOTNETS IN MALWARE DETECTION

Máté Imre SÁNTA, Norbert OLÁH

Today, cybercrime is on a massive scale, causing severe damage to both users and companies, where one of the main tools used by attackers is the malicious softwares (malware). Therefore, detecting, identifying and blocking malware is a critical security issue, as there is no genuinely comprehensive and all-encompassing solution and the field is constantly developing and changing.

Our proposed solution is a malware detection botnet capable of proper communication and data transmission. The botnet uses a Yara scanner that is able to handle and categorise our Yara rules appropriately. In order to implement a user-friendly platform, we have developed a web user interface where we can check the malwares which are caught in the quarantine. In addition, rules and rule sets based on the most common and the current "most popular" malwares have been created.

Keywords:

Security, malware, botnet, Yara, antivirus software

Kiberbiztonság - III. szekció – Intelligens környezetek

VIRTUÁLIS MÓDSZEREKKEL TÁMOGATOTT KONTROLLÁLT TESZTKÖRNYEZET KIALAKÍTÁSA TESZTPÁLYÁN FEJLETT VEZETÉSI FUNKCIÓK VIZSGÁLATÁRA

TÓTH Bálint, SZALAY Zsolt

Napjaink egyik legnagyobb járműipari kutatás-fejlesztési és validációs kihívása a fejlett vezetési funkciók megismételhető, és realisztikus módon történő tesztelése. Habár a fejlesztési fázisban a számítógépes szimulációk szerepe megnövekedett, de továbbra is szükséges a járművek próbapályán történő tesztelése valós tesztobjektumok használatával. A valós és virtuális tesztelési módszerek közötti egyensúly megtalálása kulcsfeladat. Ebben a munkában bemutatásra kerül a Scenairo-in-the-Loop (SciL) koncepció, amely a széleskörben használt SiL, HiL vagy ViL eljárásokhoz hasonló zárthurkú tesztelési módszer. A koncepció fő komponense az a vezérlőszoftver, amely a valós és virtuális zavarások vezérlését és a tesztszcenárió adaptálását végzi a tesztelt járműből és az infrastruktúrából származó bemeneti paraméterek alapján valós időben.

Kulcsszavak:

Tesztpálya, szimuláció, járműtesztelés, Scenraio-in-the-Loop

Cybersecurity - session III.– Intelligent environments

DEVELOPMENT OF A VIRTUAL TECHNIQUE AIDED, CONTROLLED TEST ENVIRONMENT ON PROVING GROUND FOR ASSESSMENT OF ADVANCED DRIVING FUNCTIONS

Bálint TÓTH, Zsolt SZALAY

Testing advanced driving functions in a highly realistic and repeatable way is one of the biggest challenges of today's automotive research, development and validation process. Although the role of the computer simulations is increasing in the development phase, it is still necessary to test the vehicles on real proving grounds with physically existing target objects. Therefore, finding the balance between the virtual and real test methods is a key task. In this paper, we present the Scenario-in-the-Loop (SciL) concept which uses similar closed-loop testing methodology compared to the widely used SiL, HiL, or ViL approaches. The core component is the control software which controls virtual and real disturbances and adapt the scenario based on the continuously changing input parameters of the tested vehicle and the proving ground infrastructure in real-time.

Keywords:
Scenario-in-the-Loop, proving ground, simulation, vehicle testing

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés

Cybersecurity - session IV.– Research and development

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés

AZ OKOS REPÜLŐTEREK KIBERBIZTONSÁGA

KATONA Gergő

Életünk számos területén találkoznunk okoseszközökön lapuló összekapcsolt rendszerekkel. Ezért ma már nem beszélhetünk különálló szigetszerűen működő rendszerekről, amiből arra következtethetünk, hogy egy szervezet rendszereinek összessége annyira biztonságos, mint a leggyengébb elektronikus információs rendszere. Ezen technológiai fejlődés, és az ebben rejlő fenyegetések a légiközlekedést sem kerülte el, mivel jelenleg is a repülőterek és légitársaságok folyamatosan integrálnak a rendszereikbe okos eszközöket, illetve mesterséges intelligenciát. Ezen magasszintű integrációval az egyes rendszerek hibái, sérülékenységei felértékelődtek. Számos támadás érte a repülési szektort, mint például több légitársaságot zsarolóvírus támadás ért, amelyek számos folyamatot értintettek és ennek hatására a járatok késtek. Ezen támadások során érzékeny adatok is nagy számban kiszivárogtak. Ezért szükséges megvizsgálni, milyen védelmi intézkedéseket kell megvizsgálni a védelem biztosítása érdekében.

Kulcsszavak:
Kiberbiztonság, okos repülőtér, kockázatok, MI

Cybersecurity - session IV.– Research and development

CYBERSECURITY OF SMART AIRPORTS

Gergő KATONA

We see systems connected to smart devices in many areas of our lives. Therefore, we can no longer talk about isolated systems, that is why we can conclude that the totality of an organisation's systems is as secure as its weakest electronic information system. This technological development and the threats it poses have not escaped the aviation sector, as airports and airlines continue to integrate smart devices and artificial intelligence into their systems. This high level of integration has amplified the flaws and vulnerabilities of individual systems. The airline industry has been hit by a number of attacks, such as the ransomware attack on several airlines, which affected many processes and caused flight delays. These attacks have also resulted in the leakage of sensitive data. It is therefore necessary to examine what security measures should be looked into to ensure protection.

Keywords:
Cybersecurity, smart airport, risks, AI

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés

KIBERVÉDELMI KÉPESSÉGEK KIALAKÍTÁSA AZ ÖNKÉNTES TARTALÉKOS ÁLLOMÁNYBAN

DEBRECENINÉ DEÁK Veronika

Magyarországon folyamatosan zajlik az önkéntes tartalékos állományba történő toborzás, amelynek oka, hogy napjaink kihívásaira történő eredményes reagálás és országunk biztonsága érdekében nélkülözhetetlen az önkéntes tartalékosok képzése, akik képesek hatékonyan támogatni a haderő munkáját és egy esetleges veszélyhelyzet bekövetkezése esetén készen állnak a beavatkozásra.

A XXI. századi hadviselés egyik legnagyobb kihívása, hogy a korábban kiforrott haditechnikák egy részét a kibertérben is alkalmazhassuk. A kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelem, valamint az arra történő felkészülés szerepét számos hazai jogszabály rögzíti. A kibertéri fenyegetések elhárításához naprakész szakmai ismeretek elsajátítására van szükség, amely megvalósulásának alapvető feltétele a magas színvonalú oktatás és képzés.

Jelen előadás célja az önkéntes tartalékos állomány kibervédelmi képességei fejlesztésének vizsgálata a kapcsolódó hazai jogszabályi környezet elemzésével. Ennek keretében javaslatot fogalmazok meg az önkéntes tartalékos állomány kibervédelmi képességeinek fejlesztésére a közszolgálati kiberbiztonsági képzés felhasználásával és kibővítésével.

Kulcsszavak:

Önkéntes tartalékos állomány, kibervédelmi képességek, kiberbiztonság, képességfejlesztés, közszolgálat

Cybersecurity - session IV.– Research and development

INTRODUCING AND IMPROVING CYBER DEFENSE CAPABILITIES IN THE VOLUNTEER RESERVE OF THE HUNGARIAN NATIONAL ARMY

Veronika DEBRECENINÉ DEÁK

Recruitment to the Voluntary Reserve of Hungarian National Army is a continuous process in Hungary. It is essential for the effective response to today's challenges of securing our country to train Volunteer Reserve personnel who can support the work of the armed forces and are ready to intervene in case of an emergency.

One of the greatest challenges of the 21st century warfare is to apply the techniques of classical warfare that have been developed in the past to the cyberspace. The importance of protection against and preparation for threats and attacks from cyberspace is laid down in multiple national laws. Countering cyberspace threats requires up-to-date professional skills, where high-quality education and training are essential.

The aim of this presentation is to examine the development of the cyber defense capabilities in the Volunteer Reserve Corps by analyzing the relevant national legislative environment. In this context, I will make a proposal for the development of the cyber defense capabilities in the Volunteer Reserve Corps reusing and expanding cyber security training for public service.

Keywords:

Volunteer reserve, cyber defense skills, cyber security, skills development, civil service

Kiberbiztonság - IV. szekció – Kutatás, fejlesztés

NEMZETKÖZI KUTATÁSOK ÁTTEKINTŐ ELEMZÉSE AZ EGYÉN INFORMÁCIÓBIZTONSÁG TUDATOSSÁGI SZINTJÉNEK MÉRÉSI MÓDSZEREIRE

BEREK László, BAK Gerda, UJHEGYI Péter, SOM Zoltán, RÉPÁS József, PETŐ Richárd

Információs társadalomban élünk, melynek gyors fejlődési üteme, a nemzetközi krízisek és konfliktusok, az egyénekre, vállalatokra, kritikus infrastruktúrákra, országokra ható növekvő kiber fenyegetettség miatt egyre fontosabb az információbiztonsági tudatosság és annak fejlesztése. A fejlesztési folyamat részeként az egyik legfontosabb kérdés, hogy mely területeken, milyen módszerekkel induljon el a lakosság és a KKV szektor információbiztonsági tudatosság fejlesztése? Fel kell mérni, hogy az elmúlt évek publikált kutatási eredményeiben, nemzetközi szinten milyen módon közelítették meg a kérdést.

Kutatásunk során magát a vizsgálatok eddigi módszertana került áttekintésre, annak érdekében, hogy a jó gyakorlatok, elterjedt mérési módszerek felkerüljenek a vizsgálati térképre. Számos lehatárolás került alkalmazásra annak érdekében, hogy csökkentsük, feldolgozható mértékűre redukáljuk a vizsgálandó publikációk számát. Publikációnkban ezért szem előtt tartjuk kutatás távlati célját, amely révén az információbiztonsági felmérések és fejlesztések eredményei elérhetővé váljanak a KKV-k számára és nemzeti szinten megjelenjenek és beépüljenek az állampolgárok edukációs programjába, az oktatásba és a hétköznapokba egyaránt, annak érdekében, hogy tájékozottabbá váljanak az információbiztonság kérdéseiben és jobban felkészüljenek a digitális világban rejlő kihívásokra.

Kulcsszavak:

Információbiztonság, felmérés, KKV, nemzetközi kutatások elemzése

Cybersecurity - session IV.– Research and development

AN OVERVIEW ANALYSIS OF INTERNATIONAL RESEARCH ON THE MEASUREMENT METHODS OF INDIVIDUAL INFORMATION SECURITY AWARENESS

László BEREK, Gerda BAK, Péter UJHEGYI, Zoltán SOM, József RÉPÁS, Richárd PETŐ

We live in an information society, where due to the rapid pace of development, international crises and conflicts, and the increasing cyber threats affecting individuals, companies, critical infrastructures, and countries, the importance of information security awareness and its development is ever increasing. As part of this process, one of the most important questions is on which areas, and by what methods, should the development of information security awareness of the population and the SME sector be initiated? It needs to be assessed how the question was approached in the published research results of recent years at an international level.

During our research, we also reviewed the methodology of the studies so far in order to include good practices and prevalent measurement methods on the research map. We applied a number of delimitations to reduce the number of publications to be examined to a manageable size. Therefore, in our publication, we keep in mind the long-term goal of our research, through which the results of information security surveys and developments will become available for SMEs and will be implemented at national level in the education programs of citizens, in education and in everyday life alike, in order to become more informed about information security issues and better prepared for the challenges of the digital world.

Keywords:

Information security, measurement, SMEs, analysis of international research

Kiberbiztonság - V. szekció – Mesterséges intelligencia és blokklánc

Cybersecurity - session V.– Artificial Intelligence and Blockchain

Kiberbiztonság - V. szekció – Mesterséges intelligencia és blokklánc

GÉPI TANULÁS ÉS MARKOV-LÁNC ALAPÚ JELSZÓGENERÁTOROK HATÉKONYSÁG VIZSGÁLATA SZÓTÁR TÁMADÁSOKHOZ

HUSZTI Andrea, OLÁH Norbert, GIRÁSZI Tamás

Neurális hálózatok sokféle alkalmazási területen játszanak fontos szerepet, és hozzájárulnak a mesterséges intelligencia térnyeréséhez. A neurális hálózatokkal lehetőség nyílik az automatizált szövegelemzésre is. A gépi tanulásnak számos etikus felhasználási módja is ismert, viszont ezek az eszközök a rosszindulatú támadók számára is elérhetőek. Az egyik ilyen lehetséges alkalmazási mód a jelszavak generálása szótár alapú támadáshoz. Számos megközelítés létezik ezeknek a kivitelezésére, ám ezek az eszközök olyan jelszó halmazokon lettek tanítva és tesztelve, hogy az adathalmaz, biztosan tartalmazott valamilyen.

A jelenlegi munkánk során megvizsgáltuk a gépi tanuló algoritmusok hatékonyságát valós adatbázisokon tanítva, valamint összevetettük a Markov láncok hatékonyságával. A különböző nyelvi sajátosságok kihatásának vizsgálata érdekében 8 ország lakosaihoz tartozó adatokat külön vizsgáltuk. Vizsgálataink alapján kiderült, hogy a gépi tanuló modellek hatásfoka jelentősen növekszik egy adott mintázattal rendelkező jelszavak esetén, viszont a valós környezetben jelentősen csökken az eredményességük.

Kulcsszavak:

Neurális hálózat, Markov-lánc, szótár, támadás, jelszó

Cybersecurity - session V.– Artificial Intelligence and Blockchain

EFFICIENT ANALYSIS OF MACHINE LEARNING AND MARKOV-BASED PASSWORD GENERATORS FOR DICTIONARY ATTACKS

Andrea HUSZTI, Norbert OLÁH, Tamás GIRÁSZI

Neural networks play an important role in a wide range of applications and are contributing to the rise of artificial intelligence. Neural networks can also be used for automated text analysis. There are many ethical uses of machine learning, but these tools are also available to malicious attackers. One such potential application is the generation of passwords for dictionary-based attacks. There are several mega-approaches to implement these, but these tools have been trained and tested on password sets such that the data set, certainly contained some

In our current work, we have investigated the efficiency of machine learning algorithms trained on real databases and compared it with the efficiency of Markov chains. In order to investigate the impact of different language features, we examined password data separately for residents of 8 countries. Our tests revealed that the efficiency of machine learning models increases significantly if a pattern given, but decreases significantly in the real environment.

Keywords:
Neural network, Markov-chain, dictionary, attack, password

Kiberbiztonság - V. szekció – Mesterséges intelligencia és blokklánc

BLOKKLÁNC ALAPÚ ALKALMAZÁS AUTOMOBIL KÖRNYEZETRE

NAGY Csaba Norbert, OLÁH Norbert

Az autóipar gyors fejlődése új kihívásokat vet fel a járművek informatikai biztonságával és adatkezelésével kapcsolatban. Számos incidens (például Kia és Tesla incidens) mutatja az alkalmazott rendszerek sérülékenységét. Az általunk javasolt megoldásban az autómobil környezet jellemzőit, biztonsági sajátosságait és követelményeit tanulmányoztunk. Megoldást dolgoztunk ki a kiber-ellenálló képesség növelésére, amelyben blokklánc alkalmazásával biztonságos identitás- és hozzáférés-kezelést (engedélyköteles blokklánc, kétfaktoros hitelesítés) és elosztott tárolást dolgoztunk ki az adatok tárolása, kezelése érdekében. Az autók szoftvereinek frissítése kritikus pont információbiztonsági szempontból. Az általunk javasolt alkalmazás figyelmezteti a felhasználót az új szoftver frissítések megjelenéséről (Over-the-Air), a rendszer komponensei lehetővé teszik a gépjárművek adatainak folyamatos frissítését, továbbá a felhasználói fiók jelszavának tárolását és ellenőrzését okosszerződések alkalmazásával.

Kulcsszavak:

IT Biztonság, blokklánc, jelszó menedzsment, járműipar, okosszerződések

Cybersecurity - session V.– Artificial Intelligence and Blockchain

BLOCKCHAIN-BASED IMPLEMENTATION FOR AUTOMOTIVE ENVIRONMENT

Csaba Norbert NAGY, Norbert OLÁH

Nowadays, the rapid development of the automotive industry poses new challenges for IT security and data management in vehicles. Numerous incidents (e.g. Kia and Tesla incidents) show the vulnerability of the vehicles. In our proposed solution, we have studied the automotive environment's characteristics, security features and requirements. We have designed a solution to enhance cyber resilience, in which we have developed a secure identity management and distributed storage using blockchain to store, manage and transmit data and passwords. Updating the software in cars is a critical point from the information security perspective. Our proposed implementation will alert the user of the release of new software updates (Over-the-Air), and the system components allow continuous updating of vehicle data, moreover, storage and validation of the user account password using smart contracts.

Keywords:
IT security, blockchain, password management, automative industry, smart contracts

Kiberbiztonság - V. szekció – Mesterséges intelligencia és blokklánc

BLOKKLÁNC ALAPÚ BIZTONSÁGI KERETRENDSZER IOT ESZKÖZÖKRE

OLÁH Norbert, NAGY Csaba Norbert

Napjainkban a különböző Internet of Things (IoT) eszközök számos alkalmazási területen jelennek meg (pl. okosváros, drónok hálózata). Azonban a biztonsági incidensek azt mutatják, hogy sérülékenyek ezek a rendszerek. Az általunk javasolt megoldásban megvizsgáltuk az IoT eszközök előnyeit és hátrányait, illetve aktuális releváns biztonsági problémákat. Megoldást kerestünk az IoT rendszerek biztonsági szintjének növelésére, amelyre a blokklánc technológiát alkalmaztuk. Az általunk javasolt keretrendszer figyelembe veszi az IoT-val kapcsolatos tervezési szempontokat (erőforrás korlátozott eszközök, skálázhatóság). Kialakítottunk egy felhasználóbarát platformot, amely képes az IoT eszközök attribútumait egy engedélyköteles blokkláncon elosztott módon tárolni. Az eszközkezelő számos funkcióval rendelkezik, melyek növelik a biztonsági követelmények magasabb szintű megvalósítását. (pl. jelszó beállítás, firmware frissítés).

Kulcsszavak:

Biztonság, IoT, blokklánc, jelszóbeállítás, firmware frissítés

Cybersecurity - session V.– Artificial Intelligence and Blockchain

BLOCKCHAIN-BASED SECURITY FRAMEWORK FOR IOT DEVICES

Norbert OLÁH, Csaba Norbert NAGY

Nowadays, various Internet of Things (IoT) devices arise in many application areas (e.g. smart city, Internet of Drones). However, security incidents show that these systems are vulnerable. In our proposed solution, we explore the advantages and disadvantages of IoT devices and current relevant security issues. We suggested a solution to increase the security level of IoT systems, for which we proposed the application of blockchain technology. Our proposed framework considers the design considerations related to IoT (resource-constrained devices, scalability). We developed a user-friendly platform for the distributed storage of IoT device attributes on a permissioned (private) blockchain. The device manager has several features to provide a higher security level and fulfil security requirements (e.g. password setting, firmware update, two-factor authentication method).

Keywords:
Security, IoT, blockchain, password setting, firmware update

Kiberbiztonság - V. szekció – Mesterséges intelligencia és blokklánc

A NAGY KOCKÁZATÚ MI RENDSZEREK KIBERBIZTONSÁGA

KOLLÁR Csaba

A nagy kockázatú MI rendszerek fejlődése a digitális korban előrevetíti a kibervédelem kiemelkedő fontosságát. Előadásom célja, hogy feltárja a nagy kockázatú MI rendszerek és a kiberbiztonság közötti összefüggéseket. A modern társadalom számos területén alkalmazzák a komplex MI rendszereket, beleértve az önvezető járműveket, az egészségügyi diagnosztikát és az okos városokat. Ezek a rendszerek adataik mélyén rejtett mintázatokat fedeznek fel, azonban a magas fokú automatizáció és összekapcsoltság kockázatot jelent a kiberbiztonságra nézve. Előadásomban olyan tényezőket mutatok be, amelyek a MI rendszerek kibervédelmi veszélyeit meghatározzák. Ilyenek a gyenge pontok és sebezhetőségek kihasználása, az adatvédelem és a magánélet megsértése, valamint az algoritmusok manipulációja. Előadásomban arra is kitérek, hogy hogyan járulhat hozzá a MI a kiberbiztonság fejlesztéséhez. Az intelligens védelmi mechanizmusok, az anomáliák észlelése és a fenyegetések előrejelzése terén az MI rendszerek nagyobb hatékonyságot és gyorsaságot kínálnak. Ugyanakkor ezeknek az eszközöknek a tervezése és bevezetése is kihívást jelent az emberi tényezők, az etika és az átláthatóság szempontjából. Az előadás végén szót ejtek az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karon működő Mesterséges Intelligencia Műhely tevékenységéről is.

Kulcsszavak:
Kiberbiztonság, mesterséges intelligencia, digitális kor, Mesterséges Intelligencia Műhely

Cybersecurity - session V.– Artificial Intelligence and Blockchain

CYBERSECURITY OF HIGH-RISK AI SYSTEMS

Csaba KOLLÁR

The evolution of high-risk AI systems in the digital age foreshadows the paramount importance of cyber security. My presentation aims to explore the links between high-risk AI systems and cybersecurity. Complex AI systems are used in many areas of modern society, including self-driving vehicles, medical diagnostics and smart cities. These systems reveal hidden patterns deep in their data, but high levels of automation and interconnectivity pose risks to cybersecurity. In my presentation, I will discuss factors that determine the cyber security risks of AI systems. These include vulnerabilities and vulnerability exploitation, data and privacy breaches, and algorithm manipulation. I will also discuss how AI can contribute to improving cybersecurity. AI systems offer greater efficiency and speed in intelligent defence mechanisms, anomaly detection and threat prediction. At the same time, the design and deployment of these tools is challenging in terms of human factors, ethics and transparency. At the end of the presentation, I will also talk about the activities of the Artificial Intelligence Workshop at the Bánki Donát Faculty of Mechanical and Safety Engineering of Óbuda University.

Keywords:
Cybersecurity, artificial intelligence, digital age, Artificial Intelligence Workshop

Kiberbiztonság - VI. szekció – Információgyűjtés és felhasználás

Cybersecurity - session VI.– Information collection and usage

Kiberbiztonság - VI. szekció – Információgyűjtés és felhasználás

ÚJ BIZTONSÁGI MESTERKÉPZÉSI SZAKOK INDÍTÁSÁNAK LEHETŐSÉGEI

KRIZSÁN Zoltán

Az alapképzésre épülő második ciklusra tervezett mesterképzés, a magasabb vezetői betöltésekhez szükséges képzettséget és végzettséget adja meg. Az alapképzési szakok tárházából figyelembe vehető szakok első sorban a mérnöki, valamint a vezetői készséget adó szakok. Az alapszak és esetleges szakirányaik közvetlen csatlakozása a lényeg. A közvetlen csatlakozás jelentése az, hogy a jelzett alapképzési szakon, szakirányon, specializáción, modulon szerzett végzettség teljes kredit értékkel vehető figyelembe a mesterképzésen. Az új mesterképzési szakot elvégző szakemberek képességeit és tudását Magyarország védelmét biztosító szervezetek és intézmények fogják hasznosítani, elsősorban a komplex védelmi feladatok megtervezése és megszervezése érdekében. A képzés célja olyan, a közszolgálati életpályára szocializálódott, a hivatásrendek közötti együttműködésre képes biztonság és védelmi igazgatási vezetők képzése, akik a közszolgálati szerveknél, az önkormányzati, a közigazgatási és a gazdasági szervezeteknél védelmi igazgatási feladatok ellátására alkalmasak. Az új módszertan és az alkalmazásra kerülő vizsgálati eszközök, kompetenciák stb. segítségével létrejött új szak tantervét meg kell tölteni képzést fejlesztő tantárgyakkal.

Kulcsszavak:
Szaklétesítés, szakindítás, kompetencia, tudás, képesség, attitűd, autonómia és felelősség

Cybersecurity - session VI.– Information collection and usage

POSSIBILITIES OF STARTING NEW SECURITY MASTER TRAINING COURSES

Zoltán KRIZSÁN

The master's program, designed for the second cycle based on the bachelor's degree, provides the training and education required for higher management positions. The majors that can be taken into account from the range of bachelor's degree programs are primarily engineering and management skills. The main thing is the direct connection of the basic course and possible specializations. The meaning of direct connection is that the degree obtained in the indicated bachelor's program, specialization, specialization, or module can be taken into account in the master's program with full credit value. The skills and knowledge of professionals completing the new master's program will be utilized by organizations and institutions that ensure the defense of Hungary, primarily for the purpose of planning and organizing complex defense tasks. The purpose of the training is to train security and defense administration managers who have been socialized into the public service career and are capable of cooperation between professional orders, who are suitable for performing defense administration tasks in public service bodies, local government, public administration and economic organizations. The new methodology and the testing tools, competencies, etc. to be applied. the curriculum of a new course created with the help of the program must be filled with subjects that develop training.

Keywords:
Specialization, competence, knowledge, ability, attitude, autonomy, responsibility.

Kiberbiztonság - VI. szekció – Információgyűjtés és felhasználás

ADATKINYERÉS CBRN HELYSZÍNELÉS SORÁN

KAKUJA Izabella

Napjainkban nem kuriózum, hogy a bűnügyi helyszín különböző veszélyes, káros vagy CBRN anyaggal szennyezett. Következésképp a helyszínen az elkövető által hátrahagyott nyomok, elváltozások, személyes tárgyak is szennyezettek lesznek. Mindezek ellenére ezen nyomok, legyenek azok hagyományos vagy digitális nyomok begyűjtésére szükség van. Abban az esetben, ha nem jelentkezik CBRN szennyezés a helyszínen, akkor lehetőség van speciális szakértelemmel rendelkező személyek bevonására, illetve a nem szennyezett digitális adathordozók laboratóriumi vizsgálatára. Abban az esetben azonban, mikor a digitális adathordozók CBRN anyaggal szennyezettek ez nem elérhető lehetőség. Először az adathordozókat meg kell tisztítani, azonban ekkor jelentkezik az a probléma, hogy eközben a hagyományos nyomok, anyagmaradványok sérülhetnek, megsemmisülhetnek. Vagyis szükség volt egy olyan módszer kialakítására, melynél a hagyományos nyomok és a digitális adatok is egyaránt megtarthatók.
Előadásomban ezt kívánom bemutatni, valamint a hagyományos és a digitális bizonyítékok helyszíni és párhuzamos begyűjtési módszerét, mely lehetővé tesz egy hatékony és gyors nyomozást, mindezt egy CBRN anyaggal terhelt környezetben.

Kulcsszavak:
CBRN anyaggal szennyezett helyszín, hagyományos és digitális bizonyíték, helyszínelés, adatkinyerés, felügyeleti lánc

Cybersecurity - session VI.– Information collection and usage

DATA EXTRACTION DURING CBRN CRIME SCENE INVESTIGATION

Izabella KAKUJA

Nowadays, it is not a curiosity that a crime scene is contaminated with various hazardous, noxious or CBRN materials. Consequently, the traces, lesions and personal effects left behind by the perpetrator at the scene will also be contaminated. To counter this, the collection of these traces, whether traditional or digital, is necessary. In the event that no CBRN contamination is found at the scene, it is possible to involve persons with specific expertise and to carry out laboratory tests on uncontaminated digital media. However, in the case of digital media contaminated with CBRN material, this is not an option. First the media must be cleaned, but then the problem arises that in the process the traditional traces and residues of the material can be damaged and destroyed. This meant that a method had to be developed whereby both traditional traces and digital data could be retained.

In my presentation, I want to show this, as well as a method for collecting both traditional and digital evidence in situ and in parallel, which allows for an efficient and fast investigation, all in a CBRN material laden environment.

Keywords:

Radiological contaminated crime scene, conventional and digital evidences, crime scene investigation, data extraction, chain of custody

Kiberbiztonság - VI. szekció – Információgyűjtés és felhasználás

A DIGITÁLIS LÁBNYOM NYOMÁBAN - OSINT TECHNIKÁK E-MAIL CÍMEK ÉS TELEFONSZÁMOK ELEMZÉSÉRE

PATAKI Norbert, HORVÁTH Barnabás

Foglalkoztatott már valaha, hogy ki lehet egy rejtélyes e-mail cím vagy telefonszám mögött valójában? Az előadás során a résztvevők megismerik, hogy hogyan kutassanak fel e-mail címeket és telefonszámokat, illetve hogyan nyerhetnek ki ezekből plusz információt. Emellett ismertetésre kerül, hogy különböző adatforrások felhasználásával hogyan azonosíthatóak be az e-mail címek és telefonszámok felhasználóinak egyéb adatai/közösségi média profiljai. Az előadás során az e-mail és telefonos adatok ellenőrzésére/gyűjtésére szolgáló OSINT eszközöket is megismerhetik az érdeklődők, melyekkel együtt különféle technikákat, illetve az ezekkel járó adatvédelmi és etikai megfontolások legjobb gyakorlatait is elsajátíthatják.

Kulcsszavak:

Kiberbiztonság, OSINT, nyílt forrású információgyűjtés

Cybersecurity - session VI.– Information collection and usage

EXPLORING THE DIGITAL FOOTPRINT - OSINT STRATEGIES FOR EMAIL AND PHONE ANALYSIS

Norbert PATAKI, Barnabás HORVÁTH

This presentation will cover the use of OSINT (Open-Source Intelligence) techniques for investigating and tracing email addresses and phone numbers. Participants will learn advanced methods for analyzing and cross-referencing different sources of data, including social media profiles, and public records, to uncover hidden connections and gain insights into individuals and organizations. The presentation will also explore various OSINT tools and techniques for verifying and validating email and phone data, as well as best practices for privacy and ethical considerations.

Keywords:
Cybersecurity, OSINT, open-source intelligence

Kiberbiztonság - VII. szekció – Egészségügy

Cybersecurity - session VII.– Healthcare

Kiberbiztonság - VII. szekció – Egészségügy

VÉSZHELYZET – EGY KÓRHÁZI OSZTÁLY POTENCIÁLIS SÉRÜLÉKENYSÉGEI

RÉPÁS József

Az egészségügyi ellátás növekvő költségei, az ellátórendszer kapacitáshiánya, az adatfüggő egészségügy korszerűtlen informatikai háttere kiemelt kiberbiztonsági kockázatot jelent. Az értékalapú ellátás felé történő elmozdulás és az új technológiák megjelenése új kihívást jelent az egészségügyi informatika számára. A betegellátás hatékonyságának növelését és a döntéshozatal támogatását célzó egészségügyi IoT eszközök (IoMT) elterjedése tovább növeli a kitettséget. Az elmúlt évek egészségügyi vonatkozású kiberbiztonsági incidensei azt mutatják, hogy az új eszközök új támadási vektorokat jelentenek, melyek kezelése mind adminisztratív, fizikai és logikai védelmi intézkedéseket igényelnek. Szükségessé válik egy olyan ajánlások kidolgozása, amely segítségével csökkenthető a kitettség. Megakadályozhatóak, megnehezíthetőek az „okos” eszközök elleni támadások, azaz az ajánlásoknak való megfelelés korlátozza a támadókat abban, hogy a világon bárhonnan hozzáférhessenek az IoMT eszközökhöz. Az IoMT specifikus biztonsági ajánlások támpontot biztosíthatnak az eszközök gyártóinak az egészségügyi környezetekbe szánt eszközök biztonsági képességeinek meghatározásához. Az egészségügyi ökoszisztéma létrehozóknak, fejlesztőinek a tervezéshez, a megfelelő eszközök kiválasztásához, konfigurálásához.

Kulcsszavak:
Kiberbiztonság, egészségügy, IoMT, ajánlás

Cybersecurity - session VII.– Healthcare

EMERGENCY ALERT - POSSIBLE VULNERABILITIES IN A HOSPITAL DEPARTMENT

József RÉPÁS

The increasing costs of health care, the lack of capacity of the care system, data-dependent healthcare, and the outdated IT background represent a major cyber security risk. The shift towards value-based care and emerging technologies present a new challenge for health informatics. The spread of healthcare IoT devices (IoMT) aimed at increasing the efficiency of patient care and supporting decision-making further increases the exposure. Healthcare-related cyber security incidents of recent years show that new devices mean new attack vectors. The management of these all requires administrative, physical, and logical protection controls. It becomes necessary to develop recommendations to reduce exposure. Attacks against "smart" devices can be prevented and made difficult, by compliance with the recommendations. It can be limiting attackers from accessing IoMT devices from anywhere in the world. The IoMT-specific security recommendations can guide device manufacturers to determine the security capabilities of devices intended for healthcare environments. Help creators and developers of the healthcare ecosystem for planning, selecting, and configuring the appropriate tools.

Keywords:
Cybersecurity, healthcare, IoMT, recommendation

Kiberbiztonság - VII. szekció – Egészségügy

MILYEN TÁMADÁSOK FENYEGETIK AZ EGÉSZSÉGÜGYI ADATOK BIZALMASSÁGÁT?

ALEXIN Zoltán

Az egészségre vonatkozó adatok a magánszféra részét képezik, ennek ellenére az önrendelkezési jogok érvényesítése gyakorlatilag lehetetlen. A jogi rendszer egyoldalú, a hatalomgyakorlás eszköze, minden jogot az állami szerveknek biztosít, az állampolgárokat pedig kiszolgáltatja a szervezeti rendszer kénye-kedvének. Az állam teljhatalmú ura a betegekről kényszerintézkedéssel összegyűjtött hatalmas adattömegnek.

Amióta „az adat az új olaj" a rendszerben megjelent a személyre szabott jogalkotás és a korrupció. Az állam folyamatosan hackeli meg (hatástalanítja) az Európai Unió jogszabályait annak érdekében, hogy ez a hatalmi helyzet érdemben ne változzon meg, sőt az állampolgároknak jogorvoslati lehetősége se legyen.

Az adatok kezelésével foglalkozó személyzet az alapvető jogok és a személyiségvédelem tekintetében képzetlen, inkompetens annak eldöntésére, hogy mi számít személyes adatnak és mi nem.

Kulcsszavak:

Egészségügyi adatok, alapvető jogok eróziója, korrupció, személyre szabott jogalkotás, szankcionálás hiánya, tájékozatlanság

Cybersecurity - session VII.– Healthcare

WHAT SORTS OF ATTACKS ARE THREATENING THE CONFIDENTIALITY OF MEDICAL DATA?

Zoltán ALEXIN

Although, personal data concerning health status are part of the private sphere, the execution of self-determination rights is practically impossible. The legal system is one-sided, it is a tool for exercising power, it grants all rights to the state bodies, and leaves the citizens at the mercy of the whims of the organizational system. The state has full authority on the huge mass of data collected on patients by the force of law.
Since when the “data is the new oil” the personalized legislation and the corruption appeared in the governance system. The state continuously hacks (neutralize) the EU legal instruments so that its power position does not change in its merit, moreover, citizens should not even have a legal remedy.
The staff dealing with data management are uneducated in fundamental rights and privacy protection, and are incompetent to decide what is considered personal data and what is not.

Keywords:
Medical data, erosion of fundamental rights, corruption, personalized legislation, lack of sanctions, unawareness

Kiberbiztonság - VII. szekció – Egészségügy

GDPR SZERINTI ADATKEZELÉS AKTUÁLIS EGÉSZSÉGÜGYI ÁGAZATI KÉRDÉSEI

NAGY István

Az Általános Adatvédelmi Rendelet (General Data Protection Regulation - GDPR) a személyes adatok védelmére vonatkozó EU-s szabályokat tartalmazza, amelyek 2018. május 25. napjától kötelezően alkalmazandók az egészségügyi intézetekben is. Az egészségügyben kiemelt figyelemmel kell kezelni a személyes adatok védelmét mivel nem csak személyes adatok, hanem különleges személyes adatok, álló és mozgó képek kerülnek rögzítésre az egészségügyi ellátások során. A tárolt adatok megőrzésére különösen hosszú megőrzési időt írnak elő az ide vonatkozó szabályok. A helyi szabályzatok és auditok naprakész felülvizsgálata és aktualizálása elkerülhetetlen.

Az előadásban tárgyalásra kerülnek a mesterséges intelligencia (MI) alkalmazása által felmerülő egészségügy centrikus adatvédelmi és kíbervédelmi kérdések. Az MI használata új kihívásokat jelent a profilalkotás és az automatikus döntéshozatal kérdéskörében.

Kulcsszavak:

GDPR, egészségügy, egészségügyi informatika, mesterséges intelligencia

Cybersecurity - session VII.– Healthcare

CURRENT HEALTHCARE INDUSTRY ISSUES OF DATA MANAGEMENT ACCORDING TO GDPR

István NAGY

The General Data Protection Regulation (GDPR) includes EU rules related the personal data's protection, which are mandatory also in the healthcare institutions from May 25, 2018. The protection of personal data must be treated with special attention in the healthcare because not only personal data but also special personal data, still and moving pictures are recorded during the health care. The relevant rules prescribe a specially long retention period for the preservation of stored data. Up-to-date review and updating of local regulations and audits are unavoidable.

Healthcare-centric data protection and cyber protection issues arising from the artificial intelligence's (AI) application are discussed in the presentation. Using of AI results new challenges in the area of profiling and automatic decision-making.

Keywords:

GDPR, healthcare, healthcare IT, artificial intelligence

Kiberbiztonság - VII. szekció – Egészségügy

REMÉLJÜK A LEGJOBBAT, TERVEZZÜK A LEGROSSZABBRA

CSORDÁS Szilárd

Az informatikai rendszerek egyre összetettebbé válnak a digitalizáció térnyerésével, és a komplexitás nem barátja a biztonságnak. Mivel egyre nagyobb a szakemberhiány, növekszik a szükségünk arra, hogy erősen támaszkodjunk a technológiára. Új generációs tűzfalakat, végpontvédelmet, eszköz nyilvántartókat, azonosítókat, sérülékenységkezelő és jogosultságkezelő rendszereket vásárolunk és használunk.

Az IT biztonsági gyártók jelentős összegeket fektetnek a fejlesztésekbe, hogy termékeik és szolgáltatásaik lépést tartsanak a támadók kreativitásával. Azonban a gyártóknak a termékeiket olyan módon kell tervezniük és építeniük, hogy azok a lehető legtöbb területen alkalmazhatók legyenek. Meg kell felelniük a kis, közepes és nagy vállalatok igényeinek és minden vállalkozásnak, intézménynek ágazattól függetlenül. Többször tapasztaltuk már, hogy milyen eltökéltek, szakmailag képzettek és erőforrásokkal rendelkező támadók léteznek. Nekik egyszer kell, hogy igazuk legyen, míg mi a védelmi oldalon nem engedhetünk meg hibát. Ha nem finomhangoljuk kellően a védelmi rendszerünket, gyakorlatilag olyan megoldást vásárolunk, ami csak az automatizált és egyszerű típusú támadások ellen nyújt védelmet. Mivel mi ismerjük a saját rendszerünket a legjobban, érdemes csapdákat és csalikat elhelyeznünk, amire a támadók nem számítanak, így azonnal észlelhetjük, ha bejutottak. Igyekezzünk preventív módon blokkolni minél több támadást, de a detektáló képesség elengedhetetlen! Nincs más választásunk, mint így csinálni!

Kulcsszavak:

Kiberbiztonság, hardening, preventív, detektív biztonság

Cybersecurity - session VII.– Healthcare

HOPE THE BEST, PLAN FOR THE WORST

Szilárd CSORDÁS

IT systems are becoming more complex with the spread of digitalization, and complexity is not friendly to security. As the shortage of cybersecurity experts grows, we need to heavily rely on technology. We purchase and use next-generation firewalls, endpoint protection, asset inventories, identity, vulnerability management, and access management systems.

IT security vendors invest significant amounts in development to ensure that their products and services keep up with attackers' creativity. However, manufacturers need to design and build their products in a way that they can be applied in as many areas as possible. They need to meet the needs of small, medium, and large companies, as well as all businesses and institutions regardless of the industry. We have experienced multiple times how determined, professionally trained attackers with resources exist. They only need to be right once, while we cannot afford any mistakes on the defense side. If we do not fine-tune our defense system properly, we essentially purchase a solution that only provides protection against automated and simple types of attacks. Since we know our own system best, it is worth placing decoys and traps that attackers do not expect, so that we can immediately detect if they have crossed the boundary.

Prevention is optimistic, detection is a must! We have no other choice!

Keywords:

Cybersecurity, hardening, preventive, detective security

Kiberbiztonság - VIII. szekció

Cybersecurity - session VIII.

Kiberbiztonság - VIII. szekció

A FELHŐBIZTONSÁG ELMÚLT 10 ÉVE A SZAKIRODALOMBAN

BAK Dorina Gerda

Az információbiztonság kritikusnak mondható mind a szervezetek, mind az egyének szempontjából. A digitális technológiák gyors terjedése átalakította azt, ahogyan élünk, dolgozunk. Ez a digitális forradalom számtalan lehetőséget hozott, de új veszélyeket is. Jelen tanulmány az információbiztonságon belül a felhőalapú szolgáltatások területén keletkezett kutatásokról nyújt áttekintést. Az elemzés alapját a 2013-2022 közötti időszakban publikált és a Scopus adatbázisában jegyzett tanulmányok kerültek be, melyekben olyan kérdésekre kerestem a választ, hogy milyen trendek figyelhetők meg a tématerületen.

Az eredmények alapján elmondható, hogy bár a felhőalapú szolgáltatások nem számítanak teljesen újnak, mégis rengeteg a nyitott kérdés és rengeteg potenciált rejt magában, amit az évről évre növekvő kutatások és publikációk is jeleznek, melyek főként az ázsiai országokban jegyeznek. A kutatások többsége az IT és computer science területén készül, azonban a téma interdiszciplináris jellegét igazolja, hogy gazdasági, oktatási és pszichológiai területen is egyre több kutatás foglalkozik a témával.

Kulcsszavak:

Kiberbiztonság, felhő, szakirodalom elemzés

Cybersecurity - session VIII.

THE LAST 10 YEARS OF CLOUD SECURITY IN THE LITERATURE

Dorina Gerda BAK

Information security is critical for both organisations and individuals. The rapid spread of digital technologies has transformed the way we live and work. This digital revolution has brought countless opportunities, but also new threats. This paper provides an overview of the research that has emerged in the field of cloud computing within information security. The analysis is based on studies published between 2013 and 2022 and listed in the Scopus database, in which I sought to answer questions such as what trends are observed in the field.

The results show that, although cloud services are not entirely new, there are still many open questions and a lot of potential, as indicated by the growing number of research papers and publications year by year, mainly in Asian countries. Most of the research is in the field of IT and computer science, but the interdisciplinary nature of the subject is confirmed by the growing number of studies in the fields of economics, education and psychology.

Keywords:

Cybersecurity, cloud, literature review,

Kiberbiztonság - VIII. szekció

PREDÁTOR FOLYÓIRATOK ÉS FÉLREVEZETŐ MÉRŐSZÁMOK - NE HAGYD, HOGY BECSAPJANAK!

BEREK László

Az online tudományos kommunikáció biztonságát leginkább veszélyeztető predátor jelenség az open access publikálás - valamint a kapcsolódó cikkeljárási díjak - elterjedésével, illetve az informatika és az internet fejlődésének hatására jelent meg. A predátor folyóiratok mellőzik a szakmai bírálatot, a plágiumellenőrzést és a publikációk minőségi vizsgálatát, az egyetlen céljuk, hogy minél több cikket jelentessenek meg, így minél nagyobb profitra tegyenek szert. Az elmúlt egy évtized során a predátor folyóiratok egy része - tökéletesítve a megtévesztés eszköztárát - nem csak a fiatal, de a tapasztalt kutatók számára is nehezen különböztethető meg a hiteles folyóiratoktól. Az elmúlt 10 év szakirodalmát vizsgálva megállapítható, hogy a predátor folyóiratok és kiadók egyre komolyabb veszélyt jelentenek az online tudományos kommunikációra. Milyen következményei lehetnek a predátor folyóiratban történő publikálásnak és milyen módon ismerhetők fel a predátor folyóiratok?

Kulcsszavak:
Predátor kiadók, predátor folyóiratok, tudománymetria, kutatói életpálya, egyetemi világranglista, tudományetika, hamis metrika

Cybersecurity - session VIII.

PREDATORY JOURNALS AND MISLEADING METRICS - DON'T LET THEM DECEIVE YOU!

László BEREK

The predatory phenomenon that poses the greatest threat to the security of online scientific communication has emerged primarily due to the proliferation of open-access publishing, along with associated article processing charges, driven by the development of information technology and the internet. Predatory journals bypass professional evaluation, plagiarism checks, and quality assessments of publications, with their sole objective being to publish as many articles as possible to maximize profit. Over the past decade, a portion of predatory journals, perfecting their arsenal of deceptive tactics, has become increasingly difficult to distinguish not only for young researchers but also for experienced ones from reputable journals. Examining the scholarly literature of the last 10 years reveals that predatory journals and publishers present an increasingly serious threat to online scientific communication. What are the consequences of publishing in predatory journals, and how can predatory journals be identified?

Keywords:
Predatory publishers, predatory jour-nals, scientometrics, career of researc-hers, university rankings, science ethics, bogus metrics

Kiberbiztonság - VIII. szekció

INFORMÁCIÓBIZTONSÁGI SZABÁLYZATOK ÁTTEKINTÉSE NEMZETKÖZI SZAKIRODALMI FELDOLGOZÁS ALAPJÁN

SOM Zoltán

Az információbiztonsági szabályzatok meglétének és érthetőségének jelentősége információbiztonsági aspektusból nem vitatható. Ezek a szabályzatok garantálják, hogy a munkaszervezet és munkavállalók gondosan kezelik és megfelelően tárolják az értékes és gyakran bizalmas információkat. Továbbá, a szabályzatok alapján a szervezetek ellenőrizhetik és igény szerint módosíthatják a saját információbiztonsági gyakorlataikat, attól függően, hogy milyen új kihívások merülnek fel az információbiztonsági környezetben. Az átlátható és jól meghatározott információbiztonsági szabályzatok hatása kiterjed a szabálykövetési hajlandóság és az információbiztonsági tudatosság, valamint a belső és külső szabálykövetési szintek javítására is. Amikor a munkatársak könnyen hozzáférhetnek a világos és érthető szabályzatokhoz, nagyobb valószínűséggel értik meg és tartják be azokat, ami csökkenti az információbiztonsági incidensek kockázatát. A megfelelően kommunikált és értelmezett szabályzatok javíthatják a munkahelyi, sőt a magánéleti információbiztonsági gyakorlatokat is. A publikációmban a szabályozásokra jellemző jó gyakorlatokat vizsgálom meg nemzetközi szakirodalom feldolgozás alapján.

Kulcsszavak:
Információbiztonsági szabályzat, információbiztonság, szabályzatértelmezés, szabálykövetési hajlandóság, információbiztonsági tudatosság

Cybersecurity - session VIII.

REVIEW OF INFORMATION SECURITY POLICIES BASED ON INTERNATIONAL LITERATURE RESEARCH

Zoltán SOM

The significance of the existence and comprehensibility of information security policies from an information security aspect is indisputable. These policies ensure that the working organization and employees handle and properly store valuable and often confidential information. Moreover, based on these policies, organizations can monitor and modify their own information security practices as needed, depending on the new challenges that arise in the information security environment. The impact of transparent and well-defined information security policies extends to the improvement of compliance willingness and information security awareness, and the enhancement of internal and external compliance levels. When colleagues can easily access clear and understandable policies, they are more likely to understand and adhere to them, which reduces the risk of information security incidents. Properly communicated and interpreted policies can improve workplace and even personal information security practices. In my publication, I examine good practices characteristic of regulations based on the processing of international professional literature.

Keywords:
Information security policy, information security, policy interpretation, compliance willingness, information security awareness

Kiberbiztonság - VIII. szekció

INFORMÁCIÓBIZTONSÁG AZ ÉPÍTŐIPARBAN

PETŐ Richárd

Családi házak, lakóépületek, irodaházak, repülőterek, katonai bázisok és egyéb állami objektumok. Több száz milliótól a száz milliárdos beruházásokig vagy tovább. Nincs olyan település, ahol ne találkozna az ember valamilyen jellegű építkezéssel. Utóbbi építkezések esetében nem ritka a 400-500 db vállalat részvétele az adott építkezésen. A jogszabályok és sok esetben a generálkivitelezők számos kötelezettséget írnak elő a munkáltatóknak (kötelező orvosi vizsgálat, munkáltatói - foglalkoztatói nyilatkozat, munkavállalói személyi adatok, tanulmányok és szakképesítések), amit teljesíteniük és a dokumentumokat át kell adniuk a generálkivitelezőnek a munkafolyamatok megkezdése előtt. A munkabalesetek kockázata ezáltal csökkenthető, de ezzel egy másik szakma kockázata (információbiztonság) pedig növekszik.
Nem ritka a generálkivitelezők körében személyi profilozás (tiltott szerek fogyasztása -alkohol, drog, …-, engedély nélküli munkavégzés, lopás, rongálás, stb. események összegyűjtése) és felhasználása. Elméletileg jószándékú felhasználás esetén a munkaterület résztvevői szűrhetőek így, de a gyakorlat sokszor eltérő. Vajon hogyan és milyen mértékben teljesülnek az adat és információbiztonsági feltételek?

Kulcsszavak:
Információbiztonság, személyes adat, különleges adat, építőipar, profilozás

Cybersecurity - session VIII.

INFORMATION SECURITY AT CONSTRUCTION SITES

Richárd PETŐ

Family house, residental buildings, business centers, airports, military bases and other government's objects. The prices start from some hundred millions to hundred milliard or more HUF. Everywhere you move you easily find a kind of construction site. In the case of lasts there are non rare that 400-500 pieces company work together. The laws and generate constructor are required obligations (such as medical documentation, pronouncement of employer, personal data, academic and qualification) in the most of case. Those requirements need to be fullfill by the empleyer before they start the work on counstruction site. The safety's risks can be reduce by this action, but it occurs risks increase of other profession (like information security). It is not rare that generate constructor takes personal profiling about workers (forbidden nervine – alcohol, drug..., working without permission, stealing, demolition, etc situation collecting) and use.

In theorically it is able to filt members of participants at using of good intent. but the practise is different.

How and how much requirement of IT security laws are fulfilled?

Keywords:

Information security, personal data, sensitive data, building industry, profiling

Kiberbiztonság - VIII. szekció

A BIOMETRIÁT HASZNÁLÓ ESZKÖZÖK ELTERJEDÉSÉNEK VIZSGÁLATA TÖBBFÉLE ASPEKTUSBÓL

UJHEGYI Péter, SOM Zoltán

A biometria témaköre nagyon szerteágazó, sok területen jelen van már és a hétköznapjokban való felhasználás egyre jobban terjed: a beszivárgó kényelmi megoldásokkal az azonosítás és hitelesítés terén. A biometrikus azonosítás technikai megoldásaival szemben számtalan elvárás, ellenérzés és félelem alakult ki, melyek hatással vannak a megoldásokra és a megoldások elterjedésére. Ezeknek a problémaköröknek feltárása és összefoglaló, elemző kutatása még kezdeti stádiumban van a tudományterületen. Ahhoz, hogy egy jó és hasznos technológiai megoldást széles körben és biztonságosan, jogszerűen tudjunk használni, szükséges vizsgálni a tényezőket és az összefüggéseket, annak érdekében, hogy mindenki számára megfelelő megoldásokat találjunk. A téma többféle szempontból vizsgálható: technológia kiválasztása, a működtető informatikai rendszer, az adatkezelés biztonsága, az információbiztonság, a jogszabályi környezet és a felhasználó egyéni szempontjai, az oktatás és a felhasználás célja is szerepet játszik egy technológia megítélésében és elterjedésében.

Kulcsszavak:
Biometria elterjedése, biometrikus azonosítás, személyes adatok védelme, információbiztonság, tudatosság, mesterséges intelligencia, jogszabályi háttér

Cybersecurity - session VIII.

EXAMINATION OF THE DISTRIBUTION OF DEVICES USING BIOMETRICS FROM SEVERAL ASPECTS

Péter UJHEGYI, Zoltán SOM

The field of biometrics is very diverse, already present in many areas. Its everyday use is increasingly spreading: with infiltrating convenience solutions in the field of identification and authentication. Against the technical solutions of biometric identification, there have been numerous expectations, reactions and fears that have affected the solutions and their propagation. The exploration and summary analysis of these complex problems are still in the initial stage in the field of science. In order to make wide use of a good and useful technological solution securely and legally, it is necessary to examine the factors and interconnections, in order to find solutions suitable for everyone. The topic can be examined from various perspectives: technology selection, the operating IT system, data management security, information security, the regulatory environment, and the user's individual aspects, as well as education and the purpose of use, all play a role in the assessment and propagation of a technology.

Keywords:
Dissemination of Biometrics, Biometric Identification, Protection of Personal Data, Information Security, Awareness, Artificial Intelligence, Legislative Background

Kiberbiztonság - IX. szekció - Diplomamunka

Cybersecurity - session IX.– Thesis

Kiberbiztonság - IX. szekció - Diplomamunka

INFORMATIKAI PROJEKTEK TERVEZÉSE A KIBERBIZTONSÁG SZEMSZÖGÉBŐL

HIS Imre

Mind a piaci, mind a védelmi szféra tekintetében elmondható, hogy az informatikai projekt feladatok komplexitása a résztvevőktől megköveteli a rendszerszintű gondolkodást, rugalmasságot, együttműködést. A projektek tervezése során az információbiztonsági szempontok nem, vagy csak későn kerülnek figyelembe vételre, ami nem biztosítja az eredménytermék szakmai szempontokon túlmutató, a szervezet sajátosságait figyelembe vevő biztonsági elvárások és jogszabályi követelmények teljesülését.

Diplomamunkám célja olyan ismeretanyag összeállítása, amely kellő segítséget nyújt az informatikai projektek tervezése esetén az információbiztonsági szempontok figyelembe vételéhez, a szereplők biztonságtudatosságának erősítéséhez.

Kutatásom speciális célja, hogy bemutassam azokat a kiberbiztonság szempontjából kulcsfontosságú tényezőket és szervezeti szempontokat, érdekeket, amelyek kiemelt jelentőséggel bírnak az informatikai rendszereket érintő projektek kivitelezése során.

Kulcsszavak:

Kiberbiztonság, projekt biztonság, biztonságtudatosság

Cybersecurity - session IX.– Thesis

PLANNING IT PROJECTS FROM THE PERSPECTIVE OF CYBERSECURITY

Imre HIS

With regard to both the market and defense spheres, it can be said that the complexity of IT project tasks requires system-level thinking, flexibility, and cooperation from the participants. During the planning of the projects, information security aspects are not taken into account, or only late, which does not ensure that the resulting product meets the security expectations and legal requirements that go beyond professional aspects and take into account the specifics of the organization.

The aim of my diploma work is to compile a knowledge base that provides sufficient assistance for taking information security aspects into account when planning IT projects, and for strengthening the security awareness of the actors. The special purpose of my research is to present the key factors and organizational aspects and interests from the point of view of cyber security, which are of particular importance during the implementation of projects involving IT systems.

Keywords:

Cybersecurity, project security, awareness

Kiberbiztonság - IX. szekció - Diplomamunka

ELLÁTÁSI LÁNCOK KIBERBIZTONSÁGÁNAK JELENTŐSÉGE

KATONA Csilla

A kibertér megerősítése, valamint a szervezetek kiberbiztonsági helyzetének javítása érdekében vált szükségessé az uniós szintű kiberbiztonsági szabályozások kiterjesztése a NIS 2 irányelvben foglaltaknak megfelelően. A kritikus infrastruktúrák kiberrezilienciájának erősítése érdekében kiemelt jelentőséggel bír továbbá a szervezetek kiberbiztonságának növelése mellett, a velük kapcsolatban álló szervezetek biztonsága is. Diplomamunkám a kiemelten kritikus szervezetek ellátási láncának kiberbiztonsági helyzetét mutatja be, különös tekintettel az egészségügyi ágazat vonatkozásaira. Azokat a tényezőket vizsgálom, amelyek hozzájárulnak a tágabb értelemben vett teljes digitális ökoszisztéma kiberbiztonságának növeléséhez, ezen túl azokat a kockázatokat szeretném feltárni, amelyek kiemelt veszélyt jelenthetnek az ágazat szereplői számára. Kutatásom célja, hogy megvizsgáljam a kiemelten kritikus szervezetek ellátási láncának kiberbiztonsági felkészültségét, mely által pontosabb kép tárul elénk a szervezetek hatékonyabb kibervédelmének eléréséhez.

Kulcsszavak:
Kibervédelem, NIS 2 irányelv, kritikus infrastruktúrák, ellátási lánc, egyészségügy

Cybersecurity - session IX.– Thesis

THE IMPORTANCE OF CYBERSECURITY IN SUPPLY CHAINS

Csilla KATONA

In order to strengthen cyberspace and improve the state of cybersecurity in organisations, it has become necessary to extend EU-wide cybersecurity regulations as set out in the NIS 2 Directive. In addition to enhancing the cybersecurity of the organisations themselves, in strengtheing the cyber resilience of critical infrastructures the security of connected organisations is of paramount importance. My thesis presents the state of cybersecurity of the supply chain of highly critical infrastructure, with a special focus on the aspects of the healthcare sector. I will examine the factors that contribute to increasing the cybersecurity of the broader digital ecosystem as a whole, and identify the risks that may pose a particular threat to the actors in the sector. The aim of my research is to examine the cybersecurity readiness of the supply chain of critical infrastructures, which will provide a more accurate picture to achieve a more effective cyber-protection of organisations.

Keywords:
Cybersecurity, NIS 2 Directive, critical infrastructures, supply chain, healthcare

Kiberbiztonság - IX. szekció - Diplomamunka

HATÉKONY BIZTONSÁGTUDATOSÍTÓ KAMPÁNYOK TERVEZÉSE

ÉRSEK Zoltán

Minden lánc olyan erős, mint a leggyengébb láncszem. A kiberbiztonságban ez a bizonyos láncszem maga az ember. A mai globalizált digitális (kiber) világban egyenszilárd, magas szintű biztonság megvalósíthatatlan az emberi tényezőből fakadó kockázatok kezelése nélkül. Az információs rendszerekre és adatokra ható humán fenyegetések leghatékonyabban biztonság tudatosítási képzésekkel csökkenthetőek. Széles kör-ben elérhető módszertanok és az arra épülő piaci szolgáltatások segítenek a negatív hatások mérséklésében, azok megelőzésé-ben. Az oktatások első lépése a tervezés, a felhasználók meglévő biztonság tudatos-sági szintjének felmérése. Az eredmények alapján készült és megvalósított oktatási tervek hatékonyságának visszamérése fontos, de a legtöbbször elhanyagolt lépés, így azok eredményessége nem kellően megalapozott. Megfelelő hangsúlyt kap az oktatás hatékonyságának és eredményes-ségének vizsgálata? Hatékony volt a kiinduló biztonságtudatosság szintjének mérése? Hogyan növelhető a hatékonyság a felméréskor? Kutatásomban ezekkel a kérdésekkel foglalkozom.

Kulcsszavak:

Kiberbiztonság, humán fenyegetés, biztonság tudatosítás

Cybersecurity - session IX.– Thesis

PLANNING EFFECTIVE SECURITY AWARENESS CAMPAIGNS

Zoltán ÉRSEK

Every chain is as strong as its weakest link. In cyber security, that particular link is the human being. In today's globalised digital (cyber) world, a consistent high level of security is impossible without addressing the human element. Human threats to information systems and data can be most effectively mitigated through security awareness training. Widely available methodologies and market services based on them help to mitigate and prevent negative impacts. The first step in training is to assess the existing security awareness level of users. Measuring back the effectiveness of the resulting and implemented education plans is an important, but often neglected step, and their effectiveness is not well established. Is there sufficient emphasis on assessing the effectiveness and efficiency of education? Was the measurement of the initial level of safety awareness effective? How can effectiveness be increased when assessing it? My research addresses these questions.

Keywords:
Cybersecurity, human threats, security awareness training

Kiberbiztonság - IX. szekció - Diplomamunka

A KRITIKUS INFRASTRUKTÚRA FONTOSSÁGÁNAK ÚJRAÉRTELMEZÉSE A COVID-19 TEKINTETÉBEN

KÁLLAI Tamás

A kritikus infrastruktúra fontosságának újraértelmezése a COVID-19 tekintetében. A kritikus infrastruktúra fogalma, történeti áttekintése, tartalmi fejlődésének vizsgálata jogszabályi környezetben a járvány alatti intézkedésekre alapozva. A COVID–19-járvány következményei és a levonható tapasztalati megállapításai a kritikus infrastruktúrához tartozó eszközök, felszerelések, nyersanyagok, késztermékek és szolgáltatások körének bővítése, továbbá az ehhez tanácsos szervezeti rendszer újra szabályozása. A járvány alatt létrehozott szervezeti újítások – mint az Operatív Törzs, a kórházparancsnoki rendszer, maszkok és védőeszközök hazai gyártásának megszervezése, felkészülés hazai oltóanyaggyártásra.

Kulcsszavak:

Kiberbiztonság, covid, kritikus infrastruktúra

Cybersecurity - session IX.– Thesis

REINTERPRETING THE IMPORTANCE OF CRITICAL INFRASTRUCTURE IN RELATION TO COVID-19

Tamás KÁLLAI

Reinterpreting the importance of critical infrastructure in relation to COVID-19. The concept of critical infrastructure, historical overview, examination of its content development in a legislative environment based on the measures taken during the epidemic. The consequences of the COVID-19 epidemic and the empirical findings that can be deduced are the expansion of the range of tools, equipment, raw materials, finished products and services belonging to critical infrastructure, as well as the re-regulation of the organizational system that is advisable for this. Organizational innovations created during the epidemic - such as the Operative Tribe, the hospital command system, the organization of the domestic production of masks and protective equipment, preparation for the domestic production of vaccines.

Keywords:
Cybersecurity, covid critical infrastructures

Kiberbiztonság - IX. szekció - Diplomamunka

KIBERTÉRI FENYEGETÉSEK FELDERÍTÉSE ELEMZÉSI PLATFORMOK HASZNÁLATÁVAL

KIRÁLY Ágnes

A digitalizációnak köszönhetően egyre nagyobb igény mutatkozik a kibertéri fenyegetések felderítésére. A fenyegetés lehet például az ellenérdekelt kibertéri szereplők azon szándéka, hogy kárt okozzanak a rendszereinkben, jelentheti azt az információt is, amely lehetővé teszi egy szervezet számára, hogy felkészüljön és megvédje a saját rendszereit, vagy adatvagyonát.

A fenyegetés elemzés hatékonyan tud hozzájárulni ahhoz, hogy egy adott szervezet megfelelően tudja csoportostani és tervezni a védelemi erőforrásait. A fenyegetettség elemzés több szinten hajtható végre. Nem ugyan azokra az információkra van szükség egy stratégiai döntés meghozatalához és egy adott rendszeren belül a támadás felismeréséhez és elhárításához. További feladat az információk feldolgozása és értelmezése, amit különböző elemző platformok segítségével végezhetünk el.

Jelen tanulmányban bemutatásra kerül, mely fenyegetettség elemzési szinteknek milyen információkra van szükség és ezeket milyen forrásból lehet beszerezni. Milyen előírások és szabályozások vannak a különböző szintű információk megosztásával kapcsolatban.

Kulcsszavak:

Kibervédelem, fenyegetés, fenyegetettségelemzés, kibertér, elemző platform

Cybersecurity - session IX.– Thesis

DETECTING CYBER THREATS USING ANALYTICS PLATFORMS

Ágnes KIRÁLY

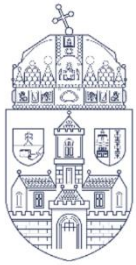
Thanks to digitalization, there is an increasing demand for the detection of cyber threats. The threat can be the intention of the adversary cyberspace actors to cause damage to our systems, it can also be the information that allows an organization to prepare and protect its own systems or data assets.

The threat analysis can effectively contribute to the fact that a given organization can properly group and plan its defense resources. Threat analysis can be performed at several levels. It is not the same data that is needed to make a strategic decision and to detect and prevent an attack within a given system. Another task is the processing and interpretation of information, which can be done with the help of various analytical platforms.

In this study, it is presented which threat analysis levels require which information and from which source they can be obtained. What are the rules and regulations regarding the sharing of different levels of information.

Keywords:

Cybersecurity, threat, threat analysis, cyberspace, analysis platform



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

BÁNKI DONÁT GÉPÉSZ ÉS
BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

BÁNKI DONÁT FACULTY OF MECHANICAL
AND SAFETY ENGINEERING

E-mail:

konferencia@alverad.hu

Web:

https://bgk.uni-obuda.hu/alverad-banki-kiberkonferencia/

https://bgk.uni-obuda.hu/en/alverad-banki-cyber-security-conference/

The conference is organized by

Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering