ALVERAD-BÁNKI NEMZETKÖZI KIBERBIZTONSÁGI ÉS KUTATÁS-FEJLESZTÉSI KONFERENCIA

ALVERAD
TECHNOLOGY FOCUS

ÓE BÁNKI

OBUDA UNIVERSITY
BÁNKI DONÁT FACULTY OF MECHANICAL AND SAFETY ENGINEERING

Alverad-Bánki International Conference on Cybersecurity and Research Development

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

ALVERAD-BÁNKI NEMZETKÖZI KIBERBIZTONSÁGI ÉS KUTATÁS-FEJLESZTÉSI KONFERENCIA

ALVERAD- BÁNKI INTERNATIONAL CYBERSECURITY AND RESEARCH & DEVELOPMENT CONFERENCE

Konferenciakötet- Book of Abstracts

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiadó / Publisher: Óbudai Egyetem, valamint
Alverad Technology Focus Kft. - Kutatás, fejlesztés és innováció Üzletág

Felelős kiadó / Editor-in-Chief: Dr. habil Farkas Tibor
Szerkesztette / Edited by: Dr. Répás József
Műszaki szerkesztő / Technical Editor: Dr. Horváth Richárd

ISBN: 978-963-449-408-9

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

KÖSZÖNTŐ

Nagy örömünkre szolgál, hogy az Európai Kiberbiztonsági Hónap keretében az Alverad Technology Focus Kft. és az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Kara megrendezte nemzetközi kiberbiztonsági és kutatás-fejlesztési konferenciáját és hogy a konferencián elhangzott előadások absztraktjai kiadvány formájában is megjelennek. A hibrid formában megvalósult rendezvény célja volt, hogy átfogó képet adjon az európai és hazai kiberbiztonsági szabályozási környezetről, annak változásairól, a mesterséges intelligencia fejlesztéshez kapcsolódó eredményekről és a digitális forenzikus vizsgálatok új eredményeinek, valamint fórumot teremtsen a legfrissebb kutatás-fejlesztési eredmények és szakmai tapasztalatok bemutatására.

A konferencia kiemelt feladatának tekintette, hogy lehetőséget biztosítson kutatók és PhD hallgatók számára tudományos eredményeinek bemutatására, fiatal kutatók egyetemi hallgatók publikációs gyakorlatának fejlesztésére, továbbá erősítse a társegyetemek, oktatók, hallgatók és szakmai partnerek közötti együttműködést. Az előadások sokszínűsége, a program gazdagsága és a szervezők szakmai elhivatottsága hozzájárult ahhoz, hogy a rendezvény valódi találkozási ponttá váljon a kiberbiztonság különböző területein dolgozó szakemberek számára.

Az előadások témaválasztása és megközelítése jól tükrözi azt a dinamikus, kihívásokkal teli környezetet, amelyben a kiberbiztonság és a kapcsolódó kutatások ma már nem csupán technológiai, hanem jogi, szervezeti és társadalmi kérdéseket is érintenek. A kötetben szereplő tanulmányok e komplexitás mentén kínálnak értékes gondolatokat, megoldási javaslatokat és kutatási irányokat.

Köszönetünket fejezzük ki minden előadónak, különösen azoknak, akiket már visszatérő előadókként köszönthettünk, valamint a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatalnak, hogy konferenciánkat támogatásban részesítette.

Hálával tartozunk mindazoknak is, akik munkájukkal, támogatásukkal és elkötelezettségükkel hozzájárultak a konferencia sikeres lebonyolításához és e kiadvány létrejöttéhez. Bízunk benne, hogy a kötet hasznos és inspiráló lesz mindazok számára, akik a kiberbiztonsághoz kapcsolódó területeken tevékenykednek.

Budapest, 2026. december 15.

Hinkel Attila
Ügyvezető

Dr. habil Farkas Tibor
Dékán

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

GREETINGS

It is our great pleasure that, within the framework of the European Cybersecurity Month, Alverad Technology Focus Ltd. and the Bánki Donát Faculty of Mechanical and Safety Engineering of Óbuda University organised their international cybersecurity and research-and-development conference, and that the abstracts of the presentations delivered at the event are now published in this volume. The hybrid conference provided an overview of European and Hungarian cybersecurity regulations, recent developments, AI-related advances, and new findings in digital forensics, while serving as a forum for sharing current research and professional experience.

The conference aimed to provide researchers and PhD students a platform to present their work, support young scholars' publication practice, and strengthen collaboration among universities and professional partners. The diverse presentations, rich programme, and dedicated organisers made it a true meeting point for cybersecurity experts.

The topics and approaches of the presentations clearly reflect the dynamic and challenging environment in which cybersecurity and related research today involve not only technological, but also legal, organisational, and societal aspects. The studies included in this volume offer valuable insights, practical solutions, and future research directions within this complex context.

We would like to express our sincere gratitude to all presenters, especially those who have returned as recurring contributors, and to the National Research, Development and Innovation Office for supporting our conference. We are also thankful to everyone whose work, support, and commitment contributed to the successful organisation of the event and to the publication of this volume. We trust that this collection will prove useful and inspiring to all those engaged in cybersecurity-related fields.

Budapest, 2025. december 15.

Attila Hinkel
CEO

Dr. habil Tibor Farkas
Dean

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Szervezőbizottság / Organizing Committee

Tiszteletbeli elnök / Honorary chair

Hinkel Attila (Alverad Technology Focus Kft.)

Általános elnök / General chair

Dr. habil Farkas Tibor (Óbudai Egyetem – ÓE BGK)

Általános társelnök / General co-chair

Dr. Horváth Richárd (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 (Nemzeti Közszolgálati Egyetem / National University of Public Service – NKE)

Dr. Alexin Zoltán (Szegedi Tudományegyetem – SZTE)

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

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

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

Dr. Krasznay Csaba (Nemzeti Közszolgálati Egyetem – NKE)

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

Dr. Török Árpád (Budapesti Műszaki Egyetem – BME)

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

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Tartalomjegyzék / Contents

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Plenáris szekció

Plenary session

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Plenáris szekció

SECTOR16 MAGYARORSZÁGI GARÁZDÁLKODÁSA

MARSI Tamás

Az ipari vezérlőrendszerek (ICS/OT) elleni támadások az utóbbi években látványosan gyakoribbá váltak, és egyre több esetben érintik a valós, fizikai folyamatokat irányító infrastruktúrákat. Az előadás bemutatja, hogy mit jelent valójában, ha egy ipari vezérlőfelület – például HMI, SCADA vagy épületautomatika – kikerül a nyílt internetre, és miért vált az ilyen kitettség a kiberfenyegetések egyik legveszélyesebb formájává. A SECTOR 16 nevű fenyegető szereplő tevékenységén keresztül áttekintjük, hogyan találhatók meg tömegesen a gyengén védett vagy nyitva hagyott távoli hozzáférések (például VNC), és miként válik egy látszólag „csak képernyőképes" kompromittáció súlyos biztonsági és reputációs incidenssé.
A hangsúly a gyakorlati reakción van: mit tegyünk az első pillanattól kezdve, hogyan történjen a gyors triage és a súlyosság megállapítása, valamint miért kulcsfontosságú az incidens azonnali bejelentése. Külön figyelmet kap a CSIRT-hálózaton alapuló gyors, hazai és nemzetközi együttműködés, valamint az események utóélete: a tanulságok levonása, a távelérés biztonságos kialakítása és az OT-környezetek védelmének megerősítése.

Kulcsszavak:

ipari vezérlőrendszerek (ICS/OT), nyílt internetes kitettség, távoli hozzáférés biztonsága, incidenskezelés és triage, CSIRT együttműködés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Plenary session

SECTOR16 ACTIVITY IN HUNGARY

Tamás MARSI

Attacks against Industrial Control Systems (ICS/OT) have become increasingly frequent in recent years, with a growing number of incidents affecting infrastructures that directly control physical processes. This presentation explores what it actually means when an industrial control interface—such as an HMI, SCADA environment, or building automation system—is exposed to the public internet, and why this type of exposure has become one of the most critical cybersecurity risks today. Using the activities of the threat actor known as SECTOR 16 as a case study, the talk highlights how weakly protected or openly accessible remote services (such as VNC) can be discovered at scale and how "just a screenshot" exposure can quickly escalate into a severe security and reputational incident. The session focuses on practical response actions: what to do from the first moment of discovery, how to perform rapid triage and assess severity, and why timely incident reporting is essential. Special emphasis is placed on fast, coordinated cooperation across national and international CSIRT networks, and on the aftermath of such incidents—drawing lessons learned, strengthening remote access practices, and improving overall security posture in OT environments.

Keywords:

industrial control systems (ICS/OT), internet exposure, remote access security, incident response and triage, CSIRT collaboration

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Plenáris szekció

ADATHASZNOSÍTÁS ÉS ADATVÉDELEM

VASS Norbert

Az adat fontossága az új technológiákkal kapcsolatban az adatszuverenitás fontosságát is felveti. Az EU az adatszuverenitást kiterjedt jogalkotással kívánja megoldani, amely újabb, egyszerűsítő jogalkotási igényt indukált mostanra. Az új technológiák jelentős változásokat okoznak a társadalomban, de ez már többször előfordult eddig. A modern technológiák nem légüres térben lebegnek, hanem a meglévő szabályok alkalmazhatóak rájuk. Az új technológiák miatt új típusú adatvédelmi problémák jelennek meg. Az adatok megfelelő védelme egyre több szakértelmet igényel, miközben egyre több adathoz egyre többen és egyre könnyebben férnek hozzá. A NAIH felügyeleti szervként, valamint az új technológiák felhasználójaként is szerepet játszik. Az adatkormányzási rendelet és az adatrendelet tárgyának összefoglalását és az Európai Adatinnovációs Testület összetételének és munkájának bemutatását követően a NAIH új technológiával kapcsolatos hatósági ügyeinek tanulságai következnek.

Kulcsszavak:

adatvédelem, NAIH, adatkormányzási rendelet, adatrendelet, mesterséges intelligencia

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Plenary session

DATA UTILISATION AND DATA PROTECTION

Norbert VASS

The importance of data in connection with new technologies also arises the issue of data sovereignty. The EU wants to address data sovereignty through extensive legislation, which has now triggered a new legislative need for simplification. New technologies are causing significant changes in society, but this has happened several times with other technologies too. Modern technologies do not float in a vacuum, but the existing rules can be applied to them. Due to new technologies, new types of data protection problems arise. Adequate protection of data requires more and more expertise, while more and more data is being accessed more and more easily by more and more people. The position of NAIH is presented as a supervisory body and also as user of new technologies. The Data Governance Act and the Data Act, and the European Data Innovation Board is discussed, as well as the lessons learned from NAIH's authority procedures.

Keywords:

data protection, NAIH, data governance act, data act, artificial intelligence

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Plenáris szekció

A NIS2 AUDITOK JELENLEGI HATÓSÁGI TAPASZTALATAI

SZEMETI Ferenc

Az előadás a NIS2 irányelv hazai végrehajtásához kapcsolódó kiberbiztonsági auditok eddigi hatósági tapasztalatait mutatja be, különös tekintettel a 7/2024. (VI. 24.) MK rendelet és a kapcsolódó végrehajtási szabályok gyakorlati alkalmazására. A tanulmány áttekinti az európai uniós és a magyar jogszabályi környezet főbb elemeit, valamint bemutatja az érintett szervezetek körét és az auditkötelezettség keletkezésének feltételeit. Részletesen elemzi az „elektronikus információs rendszer" (EIR) fogalmának jogértelmezési kérdéseit, a biztonsági osztályba sorolás szerepét, valamint az ahhoz kapcsolódó védelmi intézkedések kockázatarányos kialakítását. Az előadás ismerteti a Hatóság által tapasztalt leggyakoribb auditálási gyakorlatokat, az alkalmazható eltérések és helyettesítő védelmi intézkedések lehetőségeit, továbbá statisztikai képet ad az auditok eddigi eredményeiről. A bemutatott tapasztalatok rávilágítanak a megfelelőség javításában rejlő jelentős fejlődési potenciálra, valamint az auditok szerepére a szervezeti kiberbiztonsági érettség növelésében.

Kulcsszavak:

NIS2 irányelv, kiberbiztonsági audit, elektronikus információs rendszer (EIR), biztonsági osztályba sorolás, SZTFH hatósági tapasztalatok

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Plenary session

REGULATORY AUTHORITY EXPERIENCES FROM NIS2 CYBERSECURITY AUDITS

Ferenc SZEMETI

This paper presents the current regulatory authority experiences gained from cybersecurity audits conducted under the national implementation of the NIS2 Directive, with particular emphasis on the practical application of Government Decree 7/2024 (VI. 24) and related implementing regulations in Hungary. The study outlines the key elements of the European Union and national legal frameworks, identifies the scope of affected organisations, and clarifies the conditions under which cybersecurity audit obligations arise. Special attention is given to the legal interpretation of the concept of the Electronic Information System, the role of security classification, and the risk-based tailoring of required security measures. The paper further discusses common audit practices observed by the authority, including permissible deviations and the use of compensating security controls, and provides a statistical overview of audit outcomes to date. The findings highlight substantial opportunities for improvement in regulatory compliance and underscore the role of cybersecurity audits in enhancing organisational cybersecurity maturity.

Keywords:

NIS2 Directive, cybersecurity audit, Electronic Information System, security classification, regulatory authority experience

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Plenáris szekció

IPARI RENDSZEREK KIBERBIZTONSÁGI KIHÍVÁSAI A NIS2 MEGFELELÉS ÉRDEKÉBEN

HINKEL Attila

A NIS2 irányelv szerinti megfelelési folyamat és az első auditok gyakorlati tapasztalatai az auditor szemszögéből vegyes képet mutatnak. Az eddigi tapasztalatok rávilágítanak arra a kritikus problémára, hogy sok szervezet számára az audit az első alkalom, amikor szembesülnek a technológiai és szabályozási hiányosságaikkal, ami veszélyezteti a SZEKI>70 megfelelési küszöb elérését.

Különös hangsúlyt kap az informatikai (IT) és az ipari technológiai (OT) rendszerek közötti alapvető különbségek kezelése. Míg az IT eszközök életciklusa 1-3 év, az OT rendszerek akár 30 évig is üzemelnek, és biztonsági kontrolljaik (pl. végponti zárolás hiánya az életvédelem miatt) speciális megközelítést igényelnek. Hatékonyságot növelő lenne a NIST 800-82 szabvány alkalmazása az OT-specifikus kontrollok és kompenzációs intézkedések (pl. fizikai belépéskorlátozás) kidolgozásához.

Hangsúlyozni kell a kockázatarányos védelem fontosságát, ahol a pontos üzleti hatáselemzés és az elektronikus információs rendszerek (EIR) megfelelő szortírozása nemcsak a biztonsági szintet növeli, hanem az audit folyamatát is optimalizálja.

Kulcsszavak:

NIS2 irányelv, kiberbiztonsági audit, IT/OT konvergencia, kockázatelemzés, kompenzációs kontrollok

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Plenary session

CYBERSECURITY CHALLENGES OF INDUSTRIAL SYSTEMS IN ACHIEVING NIS2 COMPLIANCE

Attila HINKEL

The compliance process under the NIS2 Directive and the practical experiences gained from the first audits present a mixed picture from the auditor's perspective. Early experiences highlight a critical issue: for many organisations, the audit represents the first occasion on which technological and regulatory shortcomings are systematically identified, potentially jeopardising the achievement of the SZEKI>70 compliance threshold. Special emphasis is placed on addressing the fundamental differences between information technology (IT) and operational technology (OT) systems. While IT assets typically have a lifecycle of 1–3 years, OT systems may remain in operation for up to 30 years, and their security controls—such as the absence of endpoint locking due to safety-of-life considerations—require a tailored approach. The application of the NIST SP 800-82 standard could significantly enhance effectiveness in defining OT-specific controls and compensating measures, including physical access restrictions. The paper underscores the importance of risk-proportionate protection, where accurate business impact analysis and proper classification of Information Systems (IS) not only improve security posture but also optimise the audit process itself.

Keywords:

NIS2 Directive, cybersecurity audit, IT/OT convergence, risk assessment, compensating controls

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság I. Mesterséges intelligencia

Cybersecurit Session I. - Artificial Intelligence

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság I. Mesterséges intelligencia

MESTERSÉGES INTELLIGENCIA HASZNÁLATÁNAK ELŐNYEI ÉS KIHÍVÁSAI A SPIRITUÁLIS FELSŐOKTATÁSBAN

TASI István

Az előadás a mesterséges intelligencia (MI) felsőoktatásba való betörését és annak egy speciális területen, a spirituális és teológiai képzésben betöltött szerepét vizsgálja a Bhaktivedanta Hittudományi Főiskola példáján keresztül. A kutatás központi kérdése, hogyan egyeztethető össze a tradicionális értékek átadása a modern technológiai eszközökkel egy olyan környezetben, ahol az oktatás alapvetően a személyes odaadáson és a Védák által meghatározott alapvetéseken alapul.

Az intézmény a technológiai elzárkózás helyett a befogadó és kísérletező attitűd mellett döntött, felismerve az MI előnyeit az oktatás színesítésében, a kurzustervezésben és a kutatási folyamatok felgyorsításában. Az előadás konkrét példákat mutat be az MI kreatív alkalmazására, ugyanakkor rávilágít az MI használatából fakadó jelentős kockázatokra is. Kiemelt figyelmet kap az intellektuális ellustulás veszélye, a teológiai pontatlanságok (hallucinációk) jelenléte, valamint a technológia fenntarthatósági és környezetvédelmi lábnyoma.

A konklúzió hangsúlyozza, hogy bár az MI hatékony eszköz lehet a tudás közvetítésében, nem rendelkezik spirituális tudattal, így a teológiai alapelvek szerint csupán eszközként, felelősségteljes mederben tartható az oktatás folyamatában.

Kulcsszavak:

mesterséges intelligencia, teológia, vaisnavizmus, MI-napló, Bhaktivedanta Hittudományi Főiskola

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurit Session I. - Artificial Intelligence

BENEFITS AND CHALLENGES OF USING ARTIFICIAL INTELLIGENCE IN SPIRITUAL HIGHER EDUCATION

István TASI

This presentation examines the growing presence of artificial intelligence (AI) in higher education and its role within a specific domain: spiritual and theological education, illustrated through the case of the Bhaktivedanta College of Theology. The central research question addresses how the transmission of traditional values can be reconciled with modern technological tools in an educational environment fundamentally grounded in personal devotion and principles defined by the Vedic tradition. Rather than adopting technological resistance, the institution has chosen an open and experimental approach, recognising the potential benefits of AI in enriching educational practices, supporting curriculum design, and accelerating research processes. The presentation provides concrete examples of creative AI applications, at the same time, highlights significant risks associated with the use of AI. Particular attention is given to the danger of intellectual complacency, the presence of theological inaccuracies and hallucinations, as well as the sustainability and environmental footprint of AI technologies.

The conclusion emphasises that while AI can be an effective tool for knowledge transmission, it does not possess spiritual consciousness; therefore, according to theological principles, it should be applied strictly as an instrument and used responsibly within the educational process.

Keywords:

artificial intelligence, theology, Vaishnavism, AI usage log, Bhaktivedanta College of Theology

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság I. Mesterséges intelligencia

GAME OVER VAGY NEXT LEVEL? SZÁMÍTHATUNK-E A MESTERSÉGES INTELLIGENCIÁRA A KRITIKUS INFRASTRUKTÚRÁINK VÉDELMÉBEN?

SZOLNOKI Éva Gabriella

A kritikus infrastruktúrák működtetése egyre összetettebb kihívások elé néz a klímaváltozás, a digitalizáció és a hibrid fenyegetések korában. Az energia-, közlekedési és kommunikációs hálózatok biztonsága eddig főként emberi szakértelemre épült, de a növekvő komplexitás egyre inkább szükségessé teszi a mesterséges intelligencia (MI) bevonását. Az előadás áttekinti az ember–MI együttműködés előnyeit és kockázatait, különös tekintettel a bizalomra, az átláthatóságra és a döntéstámogatás szerepére. Példákon keresztül bemutatja, hogyan egészítheti ki az MI az ember döntéseit az energia-, vasúti és légiforgalmi rendszerekben. Gondolatkísérletként elemzi a 2025. április 28-i ibériai áramszünetet, és felveti, miként segíthetett volna az MI nemcsak a technikai előrejelzésben, hanem a társadalmi következmények – emberáldozatok, közlekedési káosz, pánik – mérséklésében is. Az elemzés fő üzenete, hogy a jövő reziliens infrastruktúrája nem ember vagy gép, hanem ember és gép együtt.

Kulcsszavak:

mesterséges intelligencia, kritikus infrastruktúra, reziliencia, áramszünet, társadalmi hatások

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurit Session I. - Artificial Intelligence

GAME OVER OR NEXT LEVEL? CAN WE RELY ON ARTIFICIAL INTELLIGENCE IN PROTECTING OUR CRITICAL INFRASTRUCTURES?

Éva Gabriella SZOLNOKI

Critical infrastructures face increasingly complex challenges in the age of climate change, digitalization and hybrid threats. The safety of energy, transport and communication networks has so far relied mainly on human expertise, yet the growing complexity requires the involvement of Artificial Intelligence (AI). This presentation reviews the benefits and risks of human–AI cooperation, with a special focus on trust, transparency and decision support. Through sectoral examples it illustrates how AI can complement human decision-making in energy systems, railway traffic and air traffic control. As a thought experiment, it analyses the April 28, 2025 Iberian blackout, raising the question of how AI could have helped not only in technical forecasting but also in mitigating social impacts – preventing casualties, reducing transport chaos and alleviating public panic. The main message is that the resilient infrastructures of the future will not be based on human or machine alone, but on the cooperation between the two.

Keywords:

artificial intelligence, critical infrastructure, resilience, blackout, societal impacts

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság I. Mesterséges intelligencia

KIBERBIZTONSÁGI FENYEGETÉSEK TÖBBSZINTŰ VIZSGÁLATA – A KIBERTÉRBELI KAMPÁNYOK STRUKTURÁLIS MINTÁZATAI

BALOGH Péter

A kutatás az államok kibertérbeli érdekérvényesítésének komplex formájára, a kampányok szerveződésére fókuszál. A koncepcionális keretek között vonatkozó szakirodalmi források és modellek alapján a kibertérbeli kampányokat az államok komplex módon szervezett, tartós időkeretben, számítógépes ill. online hálózati erőforrásokkal szemben megvalósított érdekérvényesítési eszközeként értelmezzük.

A vizsgálat operacionális kereteit strukturális szemléletmód jellemzi, melynek során a kibertérbeli műveletek különféle alkotóelemeinek egymás közötti viszonyait, a kapcsolódások mintázatait helyezzük az elemzések homlokterébe. A műveletek koordinálásában kulcsszerepet betöltő szereplők által a kampányokban alkalmazott eszközök köztes pozíciója kiemelt szempontként jelenik meg.

A módszertani háttér ingyenesen elérhető adatforrások (pl. MITRE ATT&CK gyűjtemények) összekapcsolásával kialakított komplex adatbázis kvantitatív másodelemzésére épül. Az adatok feldolgozása és elemzése során statisztikai módszereket és a hálózatelemzés bizonyos eljárásait alkalmaztuk.

Az adatelemzések eredményei a kibertérbeli kampányok eltérő szintű elemeinek beágyazottságára és a specifikus eszközök visszatérő jellegű alkalmazásából fakadó csomóponti integrálódási mintázataira utalnak.

Kulcsszavak:

kiberbiztonság, kibertérbeli kampányok, strukturális szemléletmód, empirikus kutatás, adatelemzés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurit Session I. - Artificial Intelligence

MULTI-LEVEL INVESTIGATION OF CYBERSECURITY THREATS – STRUCTURAL PATTERNS OF CYBERSPACE CAMPAIGNS

Péter BALOGH

The research is focusing on the complex forms of realizing state interests in the cyber sphere; the organizing patterns of campaigns.

Based on related scholarly sources and models in the conceptual framework we interpret cyberspace campaigns as complexly organized, long-term means of state advocacy targeting computer and online network resources. The operational assumptions of the investigation are characterized by a structural approach, where relationships between the various elements of cyberspace operations and the patterns of connectedness are highlighted. The intermediate position of the tools used in the campaigns by the actors playing a key role in coordinating the operations is considered an important aspect. Methodologically the research is based on quantitative secondary analysis of a complex database created by combining freely available data sources (e.g. MITRE ATT&CK collections). In the course of data analysis statistical methods and certain techniques of network analysis have been applied. The outcomes of the data analyses imply the embeddedness of the elements belonging to different levels of the cyberspace campaigns, and the clustering integration patterns resulting from the repeated use of the tools applied.

Keywords:

cybersecurity, cyberspace campaigns, structural approach, empirical research, data analysis

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság I. Mesterséges intelligencia

KIBERBŰNÖZÉS HAZAI HELYZETKÉPE RENDÉSZETI SZEMSZÖGBŐL

CSESZREGI Bálint

A kiberbűnözés elleni fellépés ma már nem csupán rendészeti feladat, hanem átfogó állami és társadalmi kihívás. A kibertérben zajló bűncselekmények jogi, gazdasági, oktatási, pszichológiai és technológiai dimenziókat is érintenek. A hatékony megelőzés és védekezés érdekében elengedhetetlen a köz- és magánszféra szoros együttműködése: a rendészeti és kormányzati szervek mellett a bankszektor, az oktatás, a technológiai vállalatok és a civil szervezetek is kulcsszereplők. Az együttműködés államhatáron belül és azon túl is szükséges, hiszen csak így akadályozható meg a bűnelkövetés és az áldozattá válás. Az előadás célja rendészeti szemszögből a védekezés, a bűncselekmények elleni fellépés, valamint trendek bemutatása.

Kulcsszavak:

kiberbűnözés, rendészeti fellépés, állami és társadalmi együttműködés, köz- és magánszféra partnerség, megelőzés és védekezés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurit Session I. - Artificial Intelligence

THE DOMESTIC CYBERCRIME LANDSCAPE FROM A LAW ENFORCEMENT PERSPECTIVE

Bálint CSESZREGI

Combating cybercrime has evolved beyond a purely law enforcement task and has become a comprehensive governmental and societal challenge. Crimes committed in cyberspace involve legal, economic, educational, psychological, and technological dimensions. Effective prevention and defence therefore require close cooperation between the public and private sectors: alongside law enforcement and governmental bodies, key stakeholders include the banking sector, educational institutions, technology companies, and civil society organisations. Such cooperation is essential both at the national and international levels, as only coordinated action can prevent criminal activity and victimisation. From a law enforcement perspective, the aim of this presentation is to provide an overview of defensive approaches, measures taken against cybercrime, and emerging trends in the cyber threat landscape.

Keywords:

cybercrime, law enforcement response, governmental and societal cooperation, public–private partnership, prevention and defence

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság I.- Mesterséges intelligencia

A MESTERSÉGES INTELLIGENCIA (AI) MEGOLDÁSOK INTEGRÁCIÓJÁNAK KIBERBIZTONSÁGI KIHÍVÁSAI

KASSAI Károly

A mesterséges intelligencia (MI) alkalmazhatósága napjainkban már nem kérdőjelezhető meg. Az MI a gazdaság, a társadalom számtalan területen beépült az életünkbe úgy, hogy már nem is érzékeljük, hogy az adott szolgáltatást MI rendszer biztosítja. Az MI rendszerek alkalmazása számtalan területen érzékeny témának számít, mint például a fegyveres erők. A prezentáció az MI katonai alkalmazás sokszínűségére, illetve a általános veszélyekre hívja fel a figyelmet. A honvédség nem csak egy-két MI rendszert kell, hogy alkalmazzon, hanem MI megoldások tucatjait, melyeket be kell integrálni a katonai információs rendszerekbe. Ezek az MI rendszerek eltérő műveleti szinteken, látnak el feladatokat, vagy ezek érdekében támogatják más rendszerek működését. A szükséges kockázatkezelés fontosabb lépéseihez mutat be támpontokat a tanulmány, támaszkodva a jogi keretrendszerre, és bevált gyakorlatokra. A testre szabott kockázatmenedzsment megalapozza a katonai szervezetek helyi, rendszerspecifikus szabályozását, melyet a meglévő kiberbiztonsági keretrendszer elemekből kell összeállítani. A vizsgálat aláhúzza, hogy az MI rendszerek a kiberbiztonsági szabályozás aló nem kaphatnak felmentést, így szükség van a meglévő eszköztár vizsgálatára, kiegészítésére és képzésekre.

Kulcsszavak:

mesterséges intelligencia (MI), katonai információs rendszer, kiberbiztonság, megbízhatóság, kockázat

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurit Session I. - Artificial Intelligence

CYBERSECURITY CHALLENGES OF THE INTEGRATION OF ARTIFICIAL INTELLIGENCE (AI) SOLUTIONS

Károly KASSAI

The applicability of artificial intelligence (AI) is no longer in question today. AI has become so integrated into countless areas of the economy and society that we no longer even notice that a given service is provided by an AI system. The use of AI systems is a sensitive issue in many areas, such as the armed forces. This presentation draws attention to the diversity of military applications of AI and the general risks involved. The armed forces need to use not just one or two AI systems, but dozens of AI solutions that must be integrated into military information systems. These AI systems perform tasks at different operational levels or support the operation of other systems for this purpose. The study provides guidance on the most important steps in the necessary risk management, based on the legal framework and best practices. Tailored risk management provides the basis for local, system-specific regulation of military organizations, which must be compiled from existing cybersecurity framework elements. The study emphasizes that AI systems cannot be exempt from cybersecurity regulations, so it is necessary to review and supplement existing tools and provide training.

Keywords:

artificial intelligence (AI), military information system, cybersecurity, trustworthiness, risk

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság II. - Kibervédelem I.

Cybersecurity Session - II. Cyber Defense I.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság II. - Kibervédelem I. Szekció

SOC ALKALMAZÁSI LEHETŐSÉGEI A NIS2 TÁMOGATÁSÁRA

ZÁMBÓ Marcell

A NIS2 irányelv bevezetése alapvető paradigmaváltást hozott a kiberbiztonság területén, amely a technikai megfelelésen túl üzleti, szervezeti és vezetői szintű felelősséget is megkövetel az érintett szervezetektől. Az előadás a kiberreziliencia új korszakát mutatja be, kiemelve a magyar megfelelési keretrendszer főbb elemeit, a vezetői elszámoltathatóság növekvő szerepét, valamint a kockázatkezelési, incidensbejelentési és ellátási lánc biztonsági követelményeket. Külön hangsúlyt kap a Security Operations Center (SOC) szerepe mint a proaktív védelem központi eleme, amely folyamatos monitorozással, incidensészleléssel és fenyegetésfelderítéssel támogatja a NIS2 megfelelést. Az előadás bemutatja a kiszervezett SOC (SOC-as-a-Service) modell előnyeit a belső SOC-építéssel szemben, valamint egy konkrét technikai architektúrán keresztül szemlélteti a naplókezelési, triage- és incidenskezelési folyamatokat. Az elemzés rámutat arra, hogy a NIS2 megfelelés nem egyszeri jogszabályi kötelezettség, hanem folyamatos, bizonyítékokon alapuló működési képesség, amely a szervezeti kiberbiztonsági érettség növelésének kulcseleme.

Kulcsszavak:

NIS2 megfelelés, kiberreziliencia, Security Operations Center (SOC), incidenskezelés és monitorozás, kiberbiztonsági audit

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity II.- Session Cyber Defence I.

PRACTICAL APPLICATIONS OF SOC CAPABILITIES FOR NIS2 COMPLIANCE

Marcell ZÁMBÓ

The introduction of the NIS2 Directive has brought about a fundamental paradigm shift in the field of cybersecurity, extending requirements beyond technical compliance to include business, organisational, and executive-level responsibilities. This presentation explores the new era of cyber resilience, highlighting the key elements of the Hungarian compliance framework, the increasing role of executive accountability, and the core requirements related to risk management, incident reporting, and supply chain security. Particular emphasis is placed on the role of the Security Operations Center (SOC) as a central pillar of proactive defence, providing continuous monitoring, incident detection, and threat intelligence to support NIS2 compliance. The presentation examines the advantages of the outsourced SOC (SOC-as-a-Service) model compared to in-house SOC implementation and illustrates logging, triage, and incident response processes through a concrete technical architecture. The analysis demonstrates that NIS2 compliance should not be regarded as a one-time regulatory obligation, but rather as a continuous, evidence-based operational capability that plays a critical role in enhancing organisational cybersecurity maturity.

Keywords:

NIS2 compliance, cyber resilience, Security Operations Center (SOC), incident response and monitoring, cybersecurity audit

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság II. - Kibervédelem I. Szekció

A MESTERSÉGES INTELLIGENCIA SZEREPE ÉS JÖVŐJE A KÖZBESZERZÉSBEN

RIPSZÁM Dóra

A mesterséges intelligencia (MI) a közbeszerzéssel több ponton is kapcsolatban áll. Az MI segítségül szolgálhat mind az ajánlattevők, mind az ajánlatkérők számára a közbeszerzési eljárások során az előkészítési szakasztól egészen a szerződés teljesítéséig. A mesterséges intelligencia korai alkalmazásával a közszféra élen járhat a technológia biztonságos, megbízható és fenntartható használatában. Azonban ez új kérdéseket is felvethet, mint például algoritmikus döntéshozatal, átláthatóság, és az emberi felelősség kérdése. Előadásomban a mesterséges intelligencia és a közbeszerzés főbb kapcsolódási pontjait tárom fel a lehetőségek és kockázatok révén.

Kulcsszavak:

mesterséges intelligencia, közbeszerzés, ajánlatkérő, ajánlattevő

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity II.- Session Cyber Defence I.

THE ROLE AND FUTURE OF ARTIFICIAL INTELLIGENCE IN PUBLIC PROCUREMENT

Dóra RIPSZÁM

Artificial intelligence (AI) is closely connected to public procurement in several respects. AI can assist both contracting authorities and tenderers throughout the procurement process - from the preparatory phase to the execution of the contract. By adopting AI technologies at an early stage, the public sector can take a leading role in ensuring the safe, reliable, and sustainable use of this technology. However, such deployment also raises new challenges, including issues of algorithmic decision-making, transparency, and human accountability. This presentation explores the main intersections between artificial intelligence and public procurement, focusing on the opportunities and risks associated with its application.

Keywords:

artificial intelligence, public procurement, contracting authority, tendere

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság II. - Kibervédelem I. Szekció

HONEYPOTOK 2.0: GÉPI TANULÁS ÉS LLM-AGENTEK A DETEKTÁLÁS, MEGTÉVESZTÉS ÉS RIPORTÁLÁS SZOLGÁLATÁBAN

ARADI Zoltán, BOTTYÁN Sándor, BÁNÁTI Anna

A honeypotok általánosságban nagy mennyiségű, úgymond „zajos” adatot tartalmazó naplófájlokat termelnek, amelyek bár tartalmazzák a legértékesebb kiberfenyegetés-adatokat, ilyen formában azonban kizárólag korlátozott interakciót kínálnak. A nagy halmazú naplóadatok feldolgozása erőforrásigényes, és elemzésük során a fals pozitív riasztások kezelése lassítja az eredményes SOC triázsolást. Tanulmányunkban egy olyan gyakorlati referencia-architektúrát javasolunk, amely a statikus adatokon a klasszikus gépi tanulást, a nyelvi feladatokban a feladatra finomhangolt LLM-eket alkalmazza a hatékonyságnövelésre. Az értékes naplóadatok kinyerését LLM-támogatással (sablonalapú adatkinyerés és zajszűrés) javítjuk, valamint az evidenciák hibrid (TF-IDF+LR/SVM/RF) detektálásának hatékonyságát finomhangolt LLM-funkciókkal növeljük. A honeypotok interakciójából fakadó támadói elköteleződést szintén LLM-funkciókkal fokozzuk, a kinyert alacsony szintű adatokat pedig tervezett funkciókkal készítjük fel a hatékony valós idejű elemzésre és a kölcsönös információmegosztásra. A hallucináció csökkentése mellett figyelmet fordítunk a legnépszerűbb MLOps/LLMOps gyakorlatokra, valamint a fő metrikák meghatározására.

Kulcsszavak:

honeypot, gépi tanulás, nagy nyelvi modellek, SOC, SIEM/SOAR/CTI

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity II.- Session Cyber Defence I.

HONEYPOTS 2.0: INTEGRATING CLASSICAL ML AND LLM AGENTS FOR DETECTION, DECEPTION, AND REPORTING

Zoltán ARADI, Sándor BOTTYÁN, Anna BÁNÁTI

Honeypots generate large log files with "noisy" data. Although these logs contain valuable cyber-threat intelligence, in their raw form they offer only limited interaction. Processing such volumes is resource-intensive, and handling false positives during analysis slows effective SOC triage. This paper proposes a practical reference architecture that uses classical machine learning for static data and task-tuned large language models (LLMs) for language-centric tasks to improve efficiency. We enhance extraction of useful log information with LLM support (template-based parsing and denoising) and increase the effectiveness of hybrid detection (TF-IDF + LR/SVM/RF) with fine-tuned LLM components. We also strengthen attacker engagement in honeypot interactions via LLM functions, and prepare low-level outputs—with planned functions—for efficient real-time analysis and reciprocal information sharing. Alongside reducing hallucination, we address common MLOps/LLMOps practices and define key metrics. The study aims to reduce handling overheads and enable longer, more meaningful sessions, leading to lower MTTD/MTTR while maintaining auditable operation.

Keywords:

honeypot, machine learning, large language models,SOC, SIEM/SOAR/CTI

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság II- Kibervédelem I.

KIBERBIZTONSÁGI FENYEGETÉSEK TÖBBSZINTŰ VIZSGÁLATA – A KIBERTÉRBELI KAMPÁNYOK STRUKTURÁLIS MINTÁZATAI

BALOGH Péter

A kutatás az államok kibertérbeli érdekérvényesítésének komplex formájára, a kampányok szerveződésére fókuszál. A koncepcionális keretek között vonatkozó szakirodalmi források és modellek alapján a kibertérbeli kampányokat az államok komplex módon szervezett, tartós időkeretben, számítógépes ill. online hálózati erőforrásokkal szemben megvalósított érdekérvényesítési eszközeként értelmezzük. A vizsgálat operacionális kereteit strukturális szemléletmód jellemzi, melynek során a kibertérbeli műveletek különféle alkotóelemeinek egymás közötti viszonyait, a kapcsolódások mintázatait helyezzük az elemzések homlokterébe. A műveletek koordinálásában kulcsszerepet betöltő szereplők által a kampányokban alkalmazott eszközök köztes pozíciója kiemelt szempontként jelenik meg.

A módszertani háttér ingyenesen elérhető adatforrások (pl. MITRE ATT&CK gyűjtemények) összekapcsolásával kialakított komplex adatbázis kvantitatív másodelemzésére épül. Az adatok feldolgozása és elemzése során statisztikai módszereket és a hálózatelemzés bizonyos eljárásait alkalmaztuk.

Az adatelemzések eredményei a kibertérbeli kampányok eltérő szintű elemeinek beágyazottságára és a specifikus eszközök visszatérő jellegű alkalmazásából fakadó csomóponti integrálódási mintázataira utalnak.

Kulcsszavak:

kiberbiztonság, kibertérbeli kampányok, strukturális szemléletmód, empirikus kutatás, adatelemzés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity II.- Session Cyber Defence I.

MULTI-LEVEL INVESTIGATION OF CYBERSECURITY THREATS – STRUCTURAL PATTERNS OF CYBERSPACE CAMPAIGNS

Péter BALOGH

The research is focusing on the complex forms of realizing state interests in the cyber sphere; the organizing patterns of campaigns. Based on related scholarly sources and models in the conceptual framework we interpret cyberspace campaigns as complexly organized, long-term means of state advocacy targeting computer and online network resources. The operational assumptions of the investigation are characterized by a structural approach, where relationships between the various elements of cyberspace operations and the patterns of connectedness are highlighted. The intermediate position of the tools used in the campaigns by the actors playing a key role in coordinating the operations is considered an important aspect. Methodologically the research is based on quantitative secondary analysis of a complex database created by combining freely available data sources (e.g. MITRE ATT&CK collections). In the course of data analysis statistical methods and certain techniques of network analysis have been applied.

The outcomes of the data analyses imply the embeddedness of the elements belonging to different levels of the cyberspace campaigns, and the clustering integration patterns resulting from the repeated use of the tools applied.

Keywords:

cybersecurity, cyberspace campaigns, structural approach, empirical research, data analysis

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság II. - Kibervédelem I. Szekció

NIS2: NYÚLÜREG A PAPÍRHEGYEKEN TÚL

BIRÓ Péter

A NIS2 irányelv (Directive (eu) 2022/2555 of the European Parliament and of the Council), a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény, valamint annak végrehajtási rendeletei együttesen határozzák meg Magyarország kibervédelmi szervezetrendszerének (beleértve az irányítási keretrendszert, a felelős intézményeket és szerveket, valamint a jogszabályokat) kereteit. A Magyarország Kiberbiztonsági Stratégiájáról szóló 1089/2025. (III. 31.) Korm. határozat azokat a stratégiai célokat fogalmazza meg, melyek alapján a digitális jólét és a nemzeti kiberbiztonsági ellenálló képesség erősíthető és fenntartható. A Nemzeti Kiberbiztonsági Akcióterv (2025–2030) a stratégiában megfogalmazott célokat bontja le végrehajtandó feladatokra, melyekkel biztosítható a Kiberbiztonsági Stratégiában foglalt célok elérése.
A jogi és szervezeti keretrendszer tehát rendelkezésre áll, van vízió, vannak stratégiai célok, ezek alapján feladatok kerültek meghatározásra, és kialakításra került egy olyan kiberbiztonsági szervezetrendszer is, mely támogatni tudja az egyes feladatok, azokon keresztül pedig a stratégia végrehajtását. A Kiberbiztonsági tv. több, mint 10 hónapos, a stratégia fél éves, így érdemes megnézni a gyakorlatban miként valósultak meg a kitűzött célok - azaz ereszkedjünk le abba a nyúlüregbe, amit a papírhegyeken túl találunk.

Kulcsszavak:

NIS2, kiberbiztonság, stratégia, hardening

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity II.- Session Cyber Defence I.

NIS2: THE RABBIT HOLE FAR FAR AWAY

Péter BIRÓ

The NIS2 Directive, the Act LXIX of 2024 on Cybersecurity of Hungary, together with its implementing decrees, jointly define the framework of Hungary's cyber defence system — including its governance structure, responsible institutions and bodies, as well as the relevant legislation. The Government Decree No. 1089/2025 (III. 31.) on the National Cybersecurity Strategy of Hungary sets forth the strategic objectives aimed at strengthening and maintaining digital prosperity and national cyber resilience. The National Cybersecurity Action Plan (2025–2030) translates the objectives defined in the Strategy into specific operational tasks, thereby ensuring the achievement of the goals established in the National Cybersecurity Strategy. Accordingly, the legal and organisational framework is in place: there is a vision, there are strategic objectives, and, based on these, concrete tasks have been defined. Furthermore, a cyber defence organisational system has been established to support the execution of these tasks, and, through them, the implementation of the Strategy itself. The Cybersecurity Act has been in force for more than ten months, and the Strategy for half a year; therefore, it is timely to examine how the set objectives have been realised in practice — to descend, so to speak, into the "rabbit hole" that lies beyond the mountain of papers.

Keywords:

NIS2, cybersecurity, strategy, hardening

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság III. - Kutatás, fejlesztés I. Szekció

Cybersecurity Session III. - Research and Developement I.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság III. - Kutatás, fejlesztés I. Szekció

VÉDELMI IGAZGATÁSI ALAPKÉPZÉSI SZAK INDÍTÁSI LEHETŐSÉGEI

KRIZSÁN Zoltán

A képzés célja olyan védelmi igazgatás szakemberek képzése, akik a Belügyminisztériumnál, a hivatásos katasztrófavédelmi szerveknél, az önkormányzati és a létesítményi tűzoltóságnál, a közigazgatási és a gazdálkodó szervezeteknél közép- és felsővezető munkakörökben képesek a védelmi feladatok tervezését, szervezését és irányítását eredményesen végrehajtani a polgári védelmi, tűzvédelmi, iparbiztonsági, önkormányzati és humánerőforrás szakterületeken. A szak elvégzését követően a hallgató megfelel a rendészeti szakvizsga követelményeinek, alkalmassá válik a hivatásos katasztrófavédelmi szervek, közigazgatási és gazdálkodó szervezetek, önkormányzatok szakmai közép- és felsőfokú vezetői beosztások betöltésére. Az alapszak és esetleges szakirányaik közvetlen csatlakozása a lényeg.
A védelmi igazgatási alapképzési szak 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 és szakirányok, majd a tantervét meg kell tölteni képzést fejlesztő tantárgyakkal, gyakorlatokkal.

Kulcsszavak:

szaklétesítés, szakindítás, kompetencia, tudás, képesség, attitűd, autonómia és felelősség

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity III. - Session Research and Developement I.

OPPORTUNITIES FOR LAUNCHING A BASIC TRAINING COURSE IN DEFENSE ADMINISTRATION

Zoltán KRIZSÁN

The aim of the training is to train defense management professionals who are capable of performing defense tasks in middle and senior management positions at the Ministry of the Interior, professional disaster management agencies, municipal and facility fire departments, administrative and economic organizations, and are able to effectively plan, organize, and manage defense tasks in the fields of civil defense, fire protection, industrial safety, municipal administration, and human resources. Upon completion of the program, students will meet the requirements of the law enforcement exam and will be qualified to fill professional middle and senior management positions in professional disaster management agencies, administrative and economic organizations, and local governments. The key point is the direct connection between the basic program and any specializations. The aim of the basic training course in defense administration is to train security and defense administration managers who are socialized into a career in public service and capable of inter-professional cooperation, who are suitable for performing defense administration tasks at public service agencies, local government, administrative, and economic organizations. New subjects and specializations created with the help of the new methodology and the testing tools, competencies, etc. to be applied, followed by filling the curriculum with training development subjects and exercises.

Keywords:

specialization, career start, competence, knowledge, skills, attitude, autonomy, and responsibility

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság III. - Kutatás, fejlesztés I. Szekció

AUTÓIPARI CAN HÁLÓZATI SÉRÜLÉKENYSÉGEK ELEMZÉSE HIBRID CYBERRANGE KÖRNYEZETBEN

KÖVESI Kristóf Zsombor, BÁNÁTI Anna

A modern járműipar gyors fejlődése egyre összetettebb elektronikus rendszereket és hálózatokat eredményez, amelyek új kihívásokat jelentenek a kiberbiztonság területén. A jelenlegi gépjárművek többsége a CAN protokollra épül, amelyen keresztül az Elektronikus Vezérlőegységek (ECU-k) kritikus adatokat cserélnek. A CAN protokoll azonban eredendően nem tartalmaz beépített biztonsági mechanizmusokat, így a modern, hálózatba kapcsolt járművek jelentős támadási felületet kínálnak a kiberfenyegetések számára. A valós CAN hálózatok elemzésére és biztonsági tesztelésére szolgáló nyílt forráskódú eszközök korlátozott elérhetősége tovább nehezíti a hatékony védelmi megoldások fejlesztését. A kutatás egy hibrid, nyílt forráskódú Cyber Range megoldást mutat be, amely virtuális járműszimulációt és fizikai ECU-kat ötvöz egy valósághű CAN hálózati környezet létrehozására. A platform lehetővé teszi CAN-alapú támadási forgatókönyvek szkriptelését, szintetikus CAN forgalom generálását, valamint a buszkommunikáció átfogó monitorozását egy dedikált Vehicle Security Operations Center (VSOC) keretében. Az eredmények hozzájárulnak a CAN-specifikus fenyegetések jobb megértéséhez, és alapot biztosítanak a következő generációs, biztonságosabb járműrendszerek fejlesztéséhez.

Kulcsszavak:

járműkiberbiztonság, Controller Area Network (CAN), elektronikus vezérlőegységek (ECU), Cyber Range, Vehicle Security Operations Center (VSOC)

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity III. - Session Research and Developement I.

ANALYSIS OF AUTOMOTIVE CAN NETWORK VULNERABILITIES IN A HYBRID CYBER RANGE ENVIRONMENT

Kristóf Zsombor KÖVESI, Anna BÁNÁTI

The rapid evolution of the modern automotive industry has resulted in increasingly complex electronic systems and networks, introducing new challenges in the field of cybersecurity. Most contemporary vehicles rely on the Controller Area Network (CAN) protocol, through which ECUs exchange critical operational data. However, the CAN protocol was not originally designed with built-in security mechanisms, making modern, network-connected vehicles a significant attack surface for cyber threats. The limited availability of open-source tools for analysing and security testing real CAN networks further complicates the development of effective defensive solutions. This research presents a hybrid, open-source Cyber Range solution that combines virtual vehicle simulation with physical ECUs to create a realistic CAN network environment. The platform enables the scripting of CAN-based attack scenarios, the generation of synthetic CAN traffic, and comprehensive bus communication monitoring within a dedicated Vehicle Security Operations Center (VSOC). The results contribute to a deeper understanding of CAN-specific threats and provide a foundation for the development of next-generation, more secure automotive systems.

Keywords:

automotive cybersecurity, Controller Area Network (CAN), Electronic Control Units (ECUs), Cyber Range, Vehicle Security Operations Center (VSOC)

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság III - Kutatás, fejlesztés I.

A MESTERSÉGES INTELLIGENCIA INTEGRÁCIÓJÁNAK KORLÁTAI A HUMÁN- ÉS TÁRSADALOMTUDOMÁNYI KÉPZÉSBEN TANULÓ HALLGATÓK KÖRÉBEN

BÁNYÁSZ-VÁCZI Kincső Boróka, RAJKI Zoltán

A mesterséges intelligencia (MI) dinamikus fejlődése és egyre szélesebb körű alkalmazása jelentős hatást gyakorol az oktatásra és a munkaerőpiacra, miközben új típusú kiberbiztonsági kockázatokat is előidéz. A kutatás célja a mesterséges intelligencia felsőoktatásban való jelenlétéhez kapcsolódó attitűdök, használati mintázatok és kockázatpercepciók vizsgálata volt, különös tekintettel a humán tudományterületeken – így a bölcsészettudományi, társadalomtudományi és pedagógusképzésekben – tanuló hallgatók körében. A kutatás alapjául egy 2023 őszén lebonyolított, 1027 fős mintán végzett online kérdőíves felmérés szolgált, amelynek eredményeit kvantitatív módszerekkel dolgozták fel a szerzők. A nemzetközi szakirodalom az MI oktatási kontextusait jellemzően a műszaki és informatikai képzések hallgatóin keresztül közelíti meg, így a humán szakterületek reprezentációja korlátozott. A kutatás hozzájárul e tudományosan alulkutatott hallgatói populáció technológiai viszonyulásának megértéséhez, és megalapozza az MI-vel kapcsolatos felsőoktatási stratégiák kidolgozását. Az empirikus eredmények elősegíthetik a humán tudományterületeken tanuló hallgatók digitális kompetenciáinak célzott fejlesztését, valamint a mesterséges intelligencia felelős és reflektív oktatási integrációját.

Kulcsszavak:

mesterséges intelligencia, felsőoktatás, kockázatészlelés, humán tudományok, kvantitatív kutatás

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity III. - Session Research and Developement I.

CHALLENGES TO THE INTEGRATION OF ARTIFICIAL INTELLIGENCE AMONG STUDENTS IN THE HUMANITIES AND SOCIAL SCIENCES

Kincső Boróka BÁNYÁSZ-VÁCZI , Zoltán RAJKI

The rapid evolution and widespread deployment of artificial intelligence (AI) significantly influence both educational frameworks and labor markets, while simultaneously introducing new cybersecurity risks. This study aimed to investigate the attitudes, usage patterns, and risk perceptions associated with the integration of AI in higher education, specifically focusing on students enrolled in humanities-related disciplines—namely, the arts, social sciences, and educational sciences. The research utilized an online questionnaire survey conducted in the autumn of 2023, with a sample size of 1,027 respondents, and analyzed the results employing quantitative methodologies. Existing international literature predominantly examines AI in educational contexts through the perspective of students in technical and IT disciplines, leading to a notable underrepresentation of humanities students in empirical research. This study aims to enhance the understanding of how this often unnoticed demographic engages with AI technologies and to establish a foundation for developing higher education strategies that address AI integration. The empirical results may facilitate the targeted enhancement of digital competencies among humanities students and encourage the responsible, reflective incorporation of AI within educational environments.

Keywords:

artificial intelligence, higher education, risk perception, humanities, quantitative research

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity III. - Session Research and Developement I.

GHOST MATH: SYSCALL-ONLY INJECTION, DETERMINISTIC SHELLCODE & QUIC C2 – A MODERN EDR BYPASS CASE STUDY

Ananda KRISHNA

This paper presents a practical case study exploring advanced evasion techniques against modern Endpoint Detection and Response (EDR) systems. The research is structured around three complementary technical pillars: (1) direct NT syscall-based process injection to bypass user-mode API hooks; (2) deterministic, mathematics-based string obfuscation aimed at defeating static analysis; and (3) a QUIC/HTTP/3-based command-and-control (C2) communication channel designed for network stealth and traffic blending. The techniques were evaluated in a Windows 11 (22H2) enterprise environment protected by CrowdStrike Falcon and Microsoft Defender for Endpoint. The results reveal observable gaps in AMSI and ETW integrity, as well as limitations in traditional API-hooking-based detection chains. In addition to offensive insights, the paper proposes practical defensive strategies, including multi-event correlation Sigma rules, module lifetime monitoring, and baseline analysis of QUIC network traffic.

Keywords:

syscall injection, EDR bypass, AMSI, ETW, QUIC C2, mathematical obfuscation

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IV.- Kutatás, fejlesztés II. Szekció

Cybersecurity Session IV. - Research and Development II.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IV.- Kutatás, fejlesztés II. Szekció

CYBER RANGE INFRASTRUKTÚRÁK A NIS2 IRÁNYELVI MEGFELELŐSÉG BIZTOSÍTÁSÁHOZ

ÉRSOK Máté, BÁNÁTI Anna

A kiberfenyegetések gyors ütemű fejlődése és komplexitása indokolttá teszi a szervezetek kiberrezilienciájának folyamatos és mérhető fejlesztését. Az Európai Unió NIS2 irányelv célja az egységesen magas szintű kiberreziliencia megteremtése, amelyhez nem elegendő kizárólag szabályozási vagy dokumentációs megfelelés: gyakorlati validációra és visszamérésre is szükség van. A tanulmány bemutatja, hogy a kibergyakorlatok – különösen a cyber range környezetekben megvalósított szimulációk – miként járulnak hozzá a NIS2 által meghatározott kulcsterületek (incidenskezelés, kockázatkezelés, üzletmenet-folytonosság, tudatosság, ellátási lánc biztonsága) fejlesztéséhez. A nemzetközi és nemzeti gyakorlatok (pl. NATO CCDCOE gyakorlatok, EU CYBER EUROPE) tapasztalatai rámutatnak arra, hogy a szerepkör-alapú, valós idejű támadásszimulációk hatékonyan támogatják a technikai, szervezeti és döntéshozatali kompetenciák fejlesztését. A kutatás amellett érvel, hogy a kibergyakorlatok automatizálhatósága, skálázhatósága és mérhetősége révén alkalmas eszközt jelentenek a NIS2-megfelelés gyakorlati értékelésére, és hidat képeznek a szabályozási elvárások és a valós működési képességek között.

Kulcsszavak:

cyber range gyakorlatok, NIS2 megfelelés, kiberreziliencia mérése, incidenskezelési szimuláció, szerepkör-alapú kibergyakorlatok

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity IV.- Session Research and Development II.

CYBER RANGE INFRASTRUCTURES FOR ACHIEVING NIS2 COMPLIANCE

Máté ÉRSOK, Anna BÁNÁTI

The rapidly evolving and increasingly complex cyber threat landscape necessitates the continuous and measurable improvement of organizational cyber resilience. The NIS2 Directive aims to establish a uniformly high level of cyber resilience across the European Union, which cannot be achieved solely through regulatory compliance but requires practical validation and operational testing. This paper examines the role of cyber exercises—particularly those conducted in cyber range environments—in supporting key NIS2 domains such as incident handling, risk management, business continuity, security awareness, and supply-chain security. Experiences from international and national exercises, including those organized within the NATO framework and EU-level cyber exercises, demonstrate that role-based, real-time attack simulations significantly enhance technical skills, organizational coordination, and decision-making under stress. The study argues that due to their scalability, repeatability, and automation potential, cyber exercises provide an effective means for assessing practical NIS2 compliance. As such, cyber range–based exercises form a critical bridge between regulatory requirements and real-world cyber defense capabilities, contributing directly to the development of resilient digital infrastructures.

Keywords:

cyber range exercises, NIS2 compliance, cyber resilience measurement, incident response simulation, role-based cyber exercises

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IV.- Kutatás, fejlesztés II. Szekció

MESTERSÉGES INTELLIGENCIÁVAL TÁMOGATOTT WEBALAPÚ ALKALMAZÁS PROMPT-FEJLESZTÉSHEZ ÉS KÉPGENERÁLÁSHOZ

ČOVIĆ Zlatko, FODOR Dávid

A mesterséges intelligencia és a webfejlesztés integrációja új lehetőségeket nyit a kreatív és technikai folyamatok automatizálásában. A kutatás célja egy olyan webalapú rendszer fejlesztése volt, amely a projektmenedzsment funkciókat mesterséges intelligencia-alapú promptfejlesztéssel és képgenerálással kapcsolja össze. A rendszer architektúrája kliens–szerver modellre épül, ahol a kommunikáció REST API-kon keresztül, JSON formátumban történik. A megoldás a ChatGPT és a Stability AI szolgáltatásait integrálja, lehetővé téve a felhasználók számára, hogy saját projektjeikhez képeket és promptokat hozzanak létre, kezeljenek és optimalizáljanak. A fejlesztés során összehasonlító elemzés is készült a korszerű képgeneráló modellek teljesítményének és alkalmazhatóságának vizsgálatára valós webes környezetben. Külön figyelmet kapott a biztonságos kulcskezelés, az authentikációs folyamatok és a hozzáférési jogosultságok szabályozása. A fejlesztés eredménye egy rugalmas, moduláris architektúra, amely demonstrálja, hogyan alkalmazható a mesterséges intelligencia a modern webes rendszerekben. A megoldás jól illeszkedik az AI-alapú oktatási és kutatási környezetekbe is.

Kulcsszavak:

mesterséges intelligencia, képgenerálás, promptfejlesztés, webfejlesztés, biztonság

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity IV.- Session Research and Development II.

AI-SUPPORTED WEB APPLICATION FOR PROMPT ENGINEERING AND IMAGE GENERATION

Zlatko ČOVIĆ, Dávid FODOR

Integrating artificial intelligence into web development opens new possibilities for automating both creative and technical processes. This research focused on designing and implementing a web-based system that combines project management functionalities with AI-driven prompt engineering and image generation. The system follows a client–server architecture, with communication handled through REST APIs using JSON format. The implemented solution integrates ChatGPT and Stability AI services, enabling users to create, manage, and optimize prompts and images for their projects. A comparative analysis evaluated the performance and applicability of state-of-the-art image generation models in real-world web environments. Special emphasis was placed on secure key management, authentication processes, and access control mechanisms. Results demonstrate that artificial intelligence can be effectively embedded into modern web systems to enhance both functionality and efficiency. Moreover, the modular architecture provides a flexible foundation for further AI-supported educational and research applications.

Keywords:

artificial intelligence, image generation, prompt engineering, web development, security

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IV.- Kutatás, fejlesztés II. Szekció

A HÁBORÚ ÚJ ARCA: POLITIKAI FILOZÓFIAI ÉS KIBERBIZTONSÁGI METSZÉSPONTOK A XXI. SZÁZADBAN

TAKÁCS Péter

A XXI. században a háború fogalma radikális szerkezetváltozáson megy keresztül. A klasszikus geopolitikai és katonai keretek mellett megjelentek az aszimmetrikus konfliktusok, a kibertérben zajló hadviselés, valamint a mesterséges intelligenciával támogatott stratégiai döntések. Kutatásom célja, hogy feltárja a háború és a politikai filozófia kölcsönhatásait: miként alakítják a hatalmi struktúrák, a szuverenitás új értelmezései és a technológiai fejlődés a modern hadviselést. Elemzésem kiterjed a kibertámadások és az információs hadviselés filozófiai dimenzióira, amelyek új normatív kérdéseket vetnek fel az államok felelőssége, az etikai szabályozás és a nemzetközi biztonsági rend fenntartása kapcsán. Az előadás rá kíván világítani arra, hogy a „háború” fogalma már nem csupán katonai konfliktusként értelmezhető, hanem a politika és technológia által formált dinamikus folyamatként.

Kulcsszavak:

háború, politikai filozófia, kiberbiztonság, információs hadviselés, szuverenitás

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity IV.- Session Research and Development II.

THE NEW FACE OF WAR: INTERSECTIONS OF POLITICAL PHILOSPOHY AND CYBERSECURITY IN THE 21.ST CENTURY

Péter TAKÁCS

In the 21st century, the concept of war is undergoing a profound structural transformation. Beyond traditional geopolitical and military frameworks, asymmetric conflicts, cyber warfare, and AI-driven strategic decision-making have emerged as central elements of modern warfare. The aim of this research is to explore the intersections of war and political philosophy, analyzing how shifts in power structures, new interpretations of sovereignty, and technological advances redefine the very nature of conflict. Particular attention is given to cyberattacks and information warfare, both of which raise novel normative questions regarding state responsibility, ethical regulation, and the stability of the international security order. This presentation seeks to demonstrate that "war" can no longer be reduced to conventional military confrontation, but must be understood as a dynamic process shaped by politics, technology, and philosophy.

Keywords:

war, political philosophy, cybersecurity, information warfare, sovereignty

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IV.- Kutatás, fejlesztés II. Szekció

TÁRSADALMI ATTITŰDÖK ÉS BIZTONSÁGI DISKURZUSOK A MESTERSÉGES INTELLIGENCIÁVAL KAPCSOLATBAN

BICZÓ Zoltán

A mesterséges intelligencia (MI) exponenciális fejlődése és széles körű társadalmi beágyazódása összetett biztonsági és bizalmi kérdéseket vet fel, különösen a kiberbiztonság kontextusában, ahol az emberi tényező – az egyének attitűdjei, hiedelmei és biztonsági tudatossága – gyakran a leggyengébb láncszemet jelenti.

Jelen tanulmány a nemzetközi szakirodalom alapján vizsgálja az MI-vel kapcsolatos társadalmi attitűdöket, percepciót és biztonsági diskurzusokat. A kockázati társadalom elméleti keretét alkalmazva elemezzük a technológiai bizalom kialakulásának mechanizmusait különböző szektorokban (egészségügy, pénzügy, ellátási láncok), különös figyelmet fordítva az oktatási szektorra, ahol a nagy nyelvi modellek új pedagógiai paradigmákat teremtenek. Eredményeink azt mutatják, hogy a társadalmi elfogadás és a biztonsági magatartás szektorfüggő, és jelentősen befolyásolja a rendszerek átláthatósága, magyarázhatósága és a döntéshozatal autonómiájának szintje. A biztonság fogalma az MI kontextusában kibővült, magában foglalva a kiberbiztonság, adatvédelem, etikai és társadalmi biztonság dimenzióit is. A médiális reprezentációk polarizált képet festenek, befolyásolva a közvéleményt, a bizalmat és a felhasználói magatartást. A tanulmány gyakorlati javaslatokat fogalmaz meg az MI-rendszerek felelősségteljes fejlesztéséhez és alkalmazásához.

Kulcsszavak:

mesterséges intelligencia, társadalmi attitűdök, kiberbiztonsági tudatosság, emberi tényező, kockázati társadalom

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity IV.- Session Research and Development II.

SOCIETAL ATTITUDES AND SECURITY DISCOURSES REGARDING ARTIFICIAL INTELLIGENCE

Zoltán BICZÓ

The exponential development and widespread societal integration of artificial intelligence (AI) raise complex security and trust issues, particularly in the context of cybersecurity, where the human factor—individuals' attitudes, beliefs, and security awareness—often represents the weakest link. Based on international literature, this study examines societal attitudes, perceptions, and security discourses related to AI. Applying the theoretical framework of risk society, we analyze the mechanisms of technological trust formation across various sectors (healthcare, finance, supply chains), with particular attention to the educational sector, where large language models are creating new pedagogical paradigms. Our findings show that societal acceptance and security behavior are sector-dependent and significantly influenced by system transparency, explainability, and the level of decision-making autonomy. The concept of security in the AI context has expanded to encompass dimensions of cybersecurity, data protection, ethical security, and societal security. Media representations paint a polarized picture, influencing public opinion, trust, and user behavior. The study formulates practical recommendations for the responsible development and application of AI systems.

Keywords:

artificial intelligence, societal attitudes, cybersecurity awareness, human factor, risk society

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IV.- Kutatás, fejlesztés II. Szekció

MINTAVÉTELEZÉSI ELJÁRÁSOK HATÁSÁNAK VIZSGÁLATA KIEGYENSÚLYOZATLAN ADATHALMAZOKON

ERDŐS Csaba

A kiegyensúlyozatlan adathalmazok kezelése központi kihívás a gépi tanulásban, mert a modellek a többségi osztály felé torzulhatnak. Bár a kiegyensúlyozó technikák elterjedtek, hatásuk az adathalmaz belső struktúrájára (zaj, átfedés) kevésbé ismert. Kutatásomban azt vizsgálom, hogyan hatnak a különböző mintavételezési eljárások a modellteljesítményre. Hipotézisem, hogy a modern, adatstruktúrát is figyelő módszerek felülmúlják a klasszikusakat, főleg zajos, átfedő adatokon. KEEL és mesterséges adathalmazokon hasonlítom össze klasszikus (például SMOTE) és modern algoritmusok hatását Döntési Fa, Random Forest és Logisztikus Regresszió modellekkel, F1-score és Balanced Accuracy metrikákat használva. Célom egy gyakorlati iránymutatás kidolgozása a megfelelő eljárás kiválasztásához, hozzájárulva a robusztusabb modellek fejlesztéséhez.

Kulcsszavak:

kiegyensúlyozatlan adathalmazok, mintavételezési technikák, gépi tanulás

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity IV.- Session Research and Development II.

EVALUATING THE IMPACT OF SAMPLING TECHNIQUES ON IMBALANCED DATASETS

Csaba ERDŐS

Handling imbalanced datasets is a central challenge in machine learning, as models tend to become biased toward the majority class. Although balancing techniques are widely used, their impact on the internal structure of the dataset (e.g., noise, class overlap) is less understood. In my research, I investigate how different sampling methods affect model performance. My hypothesis is that modern techniques, which also consider the data structure, outperform classical methods, especially on noisy and overlapping data. Using KEEL and synthetic datasets, I compare the effects of classical (e.g., SMOTE) and modern algorithms on Decision Tree, Random Forest, and Logistic Regression models, employing F1-score and Balanced Accuracy as evaluation metrics. My goal is to develop a practical guide for selecting the appropriate technique, thereby contributing to the development of more robust models.

Keywords:

unbalanced datasets, sampling techniques, machine learning

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság V.- Mesterséges intelligencia II. Szekció

Cybersecurity Session V. - Artficial Intelligence II.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság V.- Mesterséges intelligencia II. Szekció

A RENDÉSZET DIGITÁLIS ÁTALAKULÁSA: MESTERSÉGES INTELLIGENCIA ÉS KIBERBIZTONSÁG A KÖZLEKEDÉSBEN

HARANGOZÓ Valentin

A digitalizáció és a mesterséges intelligencia rohamos fejlődése alapjaiban alakítja át a közlekedés és a rendészet működését. Az okosforgalom-irányítás, az önvezető járművek és a valós idejű adatfeldolgozás új lehetőségeket kínálnak a közlekedésbiztonság javítására és a rendészeti feladatok hatékonyabb ellátására. Ugyanakkor ezzel párhuzamosan megjelennek a kiberbiztonsági kockázatok is: a közlekedési rendszerek és járművek sérülékenysége, az adatok illetéktelen hozzáférése vagy manipulálása komoly fenyegetést jelenthet a közbiztonságra.

Az előadás célja, hogy bemutassa, miként formálja át a mesterséges intelligencia a közlekedésrendészet gyakorlatát, milyen kihívásokat támaszt a kiberbiztonság terén, valamint milyen stratégiákkal és technológiai megoldásokkal lehet biztosítani a biztonságos és megbízható működést. A téma kiemelten foglalkozik a jövő rendészeti szerepével a digitális közlekedési környezetben, ahol a hatékonyság és az innováció mellett a kiberbiztonság válik a fenntartható fejlődés egyik kulcselemévé.

Kulcsszavak:

mesterséges intelligencia, kiberbiztonság, közlekedésrendészet, okos közlekedési rendszerek

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity V.- Session Artficial Intelligence II.

THE DIGITAL TRANSFORMATION OF LAW ENFORCEMENT: ARTIFICIAL INTELLIGENCE AND CYBER SECURITY IN TRANSPORTATION

Valentin HARANGOZÓ

The rapid development of digitalization and artificial intelligence is fundamentally transforming the way transportation and law enforcement operate. Smart traffic management, self-driving vehicles, and real-time data processing offer new opportunities to improve transportation safety and perform law enforcement tasks more efficiently. At the same time, however, cyber security risks are also emerging: the vulnerability of transport systems and vehicles, unauthorized access to or manipulation of data can pose a serious threat to public safety.

The aim of the presentation is to show how artificial intelligence is transforming traffic policing practices, what challenges it poses in terms of cybersecurity, and what strategies and technological solutions can be used to ensure safe and reliable operation. The topic focuses on the future role of law enforcement in the digital transport environment, where, in addition to efficiency and innovation, cybersecurity is becoming a key element of sustainable development.

Keywords:

artificial intelligence, cybersecurity, traffic policing, smart transportation systems

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság V.- Mesterséges intelligencia II. Szekció

MESTERSÉGES INTELLIGENCIA AZ IGAZSÁGÜGYI SZAKÉRTŐI MUNKÁBAN

MÁTÉ István Zsolt

Az igazságügyi informatikai szakértő munkája során, nem csupán a kiberbűncselekményekkel kapcsolatos vizsgálatok esetén kerül sor jelentős mennyiségű elektronikus adat mentésére, elemzésére és bemutatására, hanem azokban az esetekben is, ahol az elektronikus információs rendszerek az adott cselekménnyel kapcsolatos nyomok hordozójaként jelenik meg. Jól érzékelhető, hogy az így létrejövő, vagy átvett adattömeg kinyerése, elemzése, megőrzése, bemutatása és végül megsemmisítése igényli a téma részletes vizsgálatát, mely alapján az elektronikus adat életútjának egyes állomásai azonosíthatók és megfelelő módszertani keretek között felügyelhető.

Jelen tanulmány az elektronikus adatok életciklusának vizsgálatára vonatkozó kutatás első elemeként áttekintést nyújt a téma egyes részterületeiről, a jelenlegi gyakorlatokról hazai és nemzetközi viszonylatban, illetve azokról a kihívásokról, amelyek a közeli és a távoli jövőben megoldásra várnak az elektronikus adatokat kezelő hatóságok, szakértők és az infrastruktúra üzemeltetők részéről is.

Kulcsszavak:

elektronikus adat, életciklus, megőrzés, igazságügyi szakértő

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity V.- Session Artficial Intelligence II.

APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN FORENSIC EXPERT ANALYSIS

István Zsolt MÁTÉ

The digital forensic expert saves, analyses and presents a significant amount of electronic data. Some of this data is related to cybercrime, but a larger part of it is digital traces of tra-ditional crime . Obviously, the extraction, analysis, preservation, presentation and eventual destruction of the data thus generated or received requires a detailed study of the topic, which allows the identification and tracking of the stages of the life cycle of electronic data within a solid methodological framework.
As a first element of research on the life cycle of electronic data, this paper provides an overview of the different sub-areas of the subject, of national and international practices, and of the challenges that authorities, experts and infrastructure operators managing elec-tronic data will face in the near and distant future.

Keywords:

digital evidence, electronic data, lifecycle, preservation, digital forensics

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság V.- Mesterséges intelligencia II. Szekció

A MESTERSÉGES INTELLIGENCIA ALKALMAZHATÓSÁGÁNAK KORLÁTAI

FRÁTER-SZEGEDI Judit, TISZA István

Egyre szélesebb körben alkalmazzák a mesterséges intelligenciát a folyamatok automatizálására, az egyes fázisok gyorsabbá, hatékonyabbá tételére, a humán erőforrás kiváltására veszélyes munkakörökben/monoton munka esetén. A gépi tanulási megoldásokkal javítani lehet a hatékonyságot, lehetővé válik a valós idejű azonosítás, a folyamatosan fejlődő pontosság, növelhető az alkalmazkodóképesség, gyorsítható, megbízhatóbbá tehető a döntéshozatal. A tudomány mellett a mindennapi élet szerves részévé tudott válni. Internetes keresésekben, gépi fordításban, a dezinformáció elleni harcban, termékfejlesztésben, az online vásárlások folyamatainak erősítésében, a marketingben stb. nyújt megkérdőjelezhetetlen segítséget. A nyilvánvaló előnyök mellett azonban az alkalmazhatóságnak számos elméleti és gyakorlati korlátja van. A tudatosság hiánya, a tényleges gondolkodás, az egyes döntések hátterének nem ismerete, a nagyarányú hibázási lehetőség mind nagymértékben képes befolyásolni az AI hatékony működést. A legnagyobb problémát a fekete doboz jelenség okozza. A hiányosságok okán a rendszerek működtetésének alapvető feltétele a szigorú, többszintes szabályozás, az emberi felügyelet, a rendszerek használatának elsajátítása.

Kulcsszavak:

fekete doboz, adatbiztonság, alkalmazhatóság, mesterséges intelligencia, korlátok

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity V.- Session Artficial Intelligence II.

LIMITATIONS OF THE APPLICABILITY OF ARTIFICIAL INTELLIGENCE

Judit FRÁTER-SZEGEDI, István TISZA

Artificial intelligence is being used more and more widely to automate processes, make individual phases faster and more efficient, and replace human resources in dangerous jobs/monotonous work. Machine learning solutions can improve efficiency, enable real-time identification, continuously improving accuracy, increase adaptability, and make decision-making faster and more reliable. In addition to science, it has become an integral part of everyday life. It provides unquestionable help in Internet searches, machine translation, the fight against disinformation, product development, strengthening online shopping processes, marketing, etc. However, in addition to the obvious advantages, there are many theoretical and practical limitations to its applicability. Lack of awareness, actual thinking, ignorance of the background of individual decisions, and the possibility of large-scale errors can all greatly affect the effective operation of AI. The biggest problem is caused by the black box phenomenon. Due to the shortcomings, the basic conditions for operating the systems are strict, multi-level regulation, human supervision, and mastery of the use of the systems.

Keywords:

black box, data security, applicability, artifical intelligence, limits

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság V. - Mesterséges intelligencia II.

PARANCSBEFECSKENDEZÉSI TÁMADÁSOK SZIMULÁCIÓJA MESTERSÉGES INTELLIGENCIÁN ALAPULÓ IPARI VÉDELMI RENDSZEREKHEZ

DOBRÁDY Zoltán, NAGY Szilvia, HIDVÉGI Timót

Az ipari irányítórendszerek egyre nagyobb kiberbiztonsági fenyegetéseknek vannak kitéve, mivel a széles körben alkalmazott protokollok – például a Modbus RTU – nem tartalmaznak titkosítási, hitelesítési vagy integritásvédelmi mechanizmusokat. A hatékony behatolásészlelő módszerek fejlesztéséhez elengedhetetlenek a valós működést és a támadási szcenáriókat egyaránt tükröző adathalmazok. Előadásunkban egy olyan kutatási eszközt mutatunk be, amely eseményvezérelt parancsbefecskendezést tesz lehetővé valós Modbus RTU kommunikációs csatornákon. A rendszer képes a csomagok valós idejű létrehozására, befecskendezésére és megfigyelésére, miközben részletes, időbélyegzett naplókat készít. Az eszköz egyedisége abban rejlik, hogy egyszerre biztosít hardveres interakciót és támadásszimulációt, így jól reprodukálható, mesterséges intelligencia alapú behatolásészlelésre alkalmas adathalmazokat eredményez. Kutatási alkalmazásai mellett az oktatásban és biztonsági tesztelésben is hasznos eszközt kínál, elősegítve az ipari hálózatok védelmét a protokollmanipulációval szemben.

Kulcsszavak:

Ipari kiberbiztonság, Modbus RTU, parancsbefecskendezés, anomáliaészlelés, mesterséges intelligencia

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity V.- Session Artficial Intelligence II.

SIMULATING COMMAND INJECTION ATTACKS FOR AI-BASED PROTECTION OF INDUSTRIAL PROTOCOLS

Zoltán DOBRÁDY, Szilvia NAGY, Timót HIDVÉGI

Industrial control systems continue to face rising cybersecurity risks, as many widely deployed protocols, such as Modbus RTU, lack encryption, authentication, or integrity mechanisms. To support the development of robust intrusion detection methods, realistic datasets reflecting both normal operations and malicious scenarios are essential. In this work, we introduce a research tool that enables event-driven command injection against real Modbus RTU communication channels. The platform allows users to craft, inject, and monitor packets in real time, while automatically recording detailed, timestamped logs. This dual capability of interacting with physical hardware and simulating cyberattacks provides a unique foundation for generating reproducible datasets suitable for training machine learning–based detection systems. Beyond research, the tool also offers value for education, security testing, and benchmarking of AI-driven anomaly detection strategies, helping to advance the protection of industrial networks against protocol manipulation.

Keywords:

industrial cybersecurity, modbus RTU, command injection, anomaly detection, machine learning

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság V.- Mesterséges intelligencia II. Szekció

MESTERSÉGES INTELLIGENCIA ALKALMAZÁSA HONEYPOT RENDSZEREKBEN

GONDA Ábel

A közigazgatás önmagában egy egyedi jellemzőkkel ellátott szektor, amely különleges szükségleteket igényel ha kiberbiztonságról beszélünk. 2018 óta a Nemzeti Kibervédelmi Intézet szolgáltatási palettájában megtalálható a Honeypot azaz Csapdarendszer is. Ez a különleges rendszer képes egyedülálló megoldásokkal eltéríteni a behatolókat, az általuk visszahagyott adatokat pedig felhasználni kiberhírszerzési és trend elemzési folyamatokban. Az előadás során a hallgatóság egy rövid betekintést nyerhet a Honeypotok világába és ezen rendszerek stratégiai felhasználásában az NKI által.

Kulcsszavak:

csapdarendszerek, közigazgatás, Nemzeti Kibervédelmi Intézet, kiberhírszerzés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity V.- Session Artficial Intelligence II.

THE USECASE OF HONEYPOTS IN THE PUBLIC ADMINISTRATION SECTOR

Ábel GONDA

The public administration by itself contains many unique features, which certainly demands special needs in the world of cybersecurity. Since 2018 the National Cyber Security Center (NCSC) Hungary has Honeypots in their range of services. This specialized network security system uses some unique ways to keep intruders busy and utilize interaction data for cyber intelligence and trends analyzis. In this session the audience will be able to get a quick glance into the world of Honeypot and their strategic use by the NCSC.

Keywords:

honeypots, public administration, National Cyber Security Center, cyber intelligence

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VI. - Ipari kiberbiztonság Szekció

Cybersecurity Session VI. - Operation Technology

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VI.- Ipari kiberbiztonság Szekció

KÉPZÉSEK ÉS TOVÁBBKÉPZÉSEK RENDSZERE AZ KIBERBIZTONSÁGI JOGSZABÁLYOK ALAPJÁN

OROSHÁZI Dávid

Az előadás a hazai kiberbiztonsági jogszabályi környezethez illeszkedő képzési és továbbképzési rendszer átfogó bemutatására vállalkozik, különös tekintettel a NIS2 irányelv hazai átültetésére és az ahhoz kapcsolódó végrehajtási rendeletekre. A tanulmány elemzi a 7/2024. (VI. 24.) MK rendelet, a 17/2025. (VII. 24.) EM rendelet, valamint a kapcsolódó kormányrendeletek és törvényi előírások által meghatározott képzési kötelezettségeket. Részletesen tárgyalja a belső tudatossági képzések és a külső, szervezett képzések rendszerét, a vezetők és információbiztonsági felelősök (IBF) számára előírt követelményeket, továbbá az elfogadható képesítések és továbbképzések struktúráját. Az előadás kitér a mentességi szabályokra, az átmeneti rendelkezésekre, valamint a képző intézményekkel szemben támasztott szakmai és jogi elvárásokra is. A bemutatott rendszer célja a kiberbiztonsági kompetenciák egységes, ellenőrizhető és fenntartható fejlesztése a szabályozott szervezetek körében.

Kulcsszavak:

kiberbiztonsági képzések, NIS2 irányelv, információbiztonsági felelős, továbbképzési kötelezettség, jogszabályi megfelelés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VI.- Operation Technology

SYSTEM OF TRAINING AND CONTINUING PROFESSIONAL DEVELOPMENT BASED ON CYBERSECURITY LEGISLATION

Dávid OROSHÁZI

This paper provides a comprehensive overview of the training and continuing professional development framework defined by the Hungarian cybersecurity regulatory environment, with particular emphasis on the national implementation of the NIS2 Directive and its related executive regulations. The study examines the requirements set out in Government Decree 7/2024 (VI. 24), Ministerial Decree 17/2025 (VII. 24), and the associated legislative acts governing cybersecurity education and professional training obligations. Special attention is given to the distinction between internal awareness-raising training programmes and externally organised training schemes, including the mandatory requirements for executive management and Information Security Officers (ISOs). The paper also analyses the system of recognised qualifications, continuing education requirements, exemption rules, and transitional provisions. Furthermore, it outlines the professional and legal criteria applicable to training providers operating within the formal adult education framework. The presented regulatory model aims to ensure a structured, verifiable, and sustainable development of cybersecurity competencies across regulated organisations, supporting compliance, resilience, and organisational preparedness in an evolving threat landscape.

Keywords:

cybersecurity training, NIS2 Directive, information security officer, continuing professional development, regulatory compliance

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VI.- Ipari kiberbiztonság Szekció

TESZTKÖRNYEZET OT OKTATÁSHOZ ÉS EXPLOITOK FEJLESZTÉSÉHEZ

HIDVÉGI Timót

A kritikus infrastruktúrák egyik területe az ipari hálózat (Operational Technology, OT), amely különböző ipari eszközökből épül fel. Ezek az eszközök (pl.: PLC, HMI) nagyon sérülékenyek, és olyan protokollok segítségével kommunikálnak, amelyek könnyen támadhatók. Az ipari hálózatok védelme nagyon fontos, és ehhez ismerni kell az OT rendszerek felépítését, működését. Ma már a védelmet segíti a Mesterséges Intelligencia, illetve még a honeypot-ok is. Elkészült egy olyan tesztkörnyezet, amelynek a segítségével könnyen lehet tanítani az OT hálózatokban megtalálható informatikai architektúrát a mérnökhallgatóknak és az informatikusoknak. A hordozható tesztmodell egy 19”-os rackpolcon kapott helyet. Megtalálhatók itt a különböző gyártók PLC-éi, amelyeket ma is nagyon sok helyen alkalmaznak. A tesztkörnyezet alkalmazásával a különböző ipari protokollok és több támadási módszer is megismerhető. A tesztkörnyezet tartalmaz még mikroszámítógépeket is. Ezeken a számítógépeken Ubuntu Server operációs rendszer van, és segítik a különböző kommunikációs protokollok alkalmazását és még az egyedi script-ek fejlesztését is. A mikroszámítógépek segítségével implementálhatók Modbus TCP, S7, OPC-UA, Ethernet/IP protokollok, de akár honeypot-ok is.
A tesztkörnyezet előnye, hogy alkalmas Machine Learning modellek, kártékony kódok és exploit-ok fejlesztésére is.

Kulcsszavak:

iparbiztonság, Modbus TCP, MiTM, anomáliák detektálása, gépi tanulás

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VI.- Operation Technology

TEST ENVIRONMENT FOR EDUCATION AND EXPLOIT DEVELOPMENT

Timót HIDVÉGI

An area of critical infrastructure is the industrial network (Operational Technology, OT), which is made up of various industrial devices. These devices (e.g., PLC, HMI) are very vulnerable and communicate using protocols that are easily attacked. Protecting industrial networks is very important, and this requires knowledge of the structure and operation of OT systems. Today, protection is aided by artificial intelligence and even honeypots. A test environment has been created that can be used to easily teach engineering students and computer scientists about the IT architecture found in OT networks. The portable test model is hosted in a 19" rack shelf. It contains PLCs from various manufacturers, which are still widely used today. The test environment can be used to learn about different industrial protocols and multiple attack methods. The test environment also includes some microcomputers. The Ubuntu Server operating system run on these computers and support the use of various communication protocols and even the development of custom scripts. Microcomputers can be used to implement Modbus TCP, S7, OPC-UA, Ethernet/IP protocols, and even honeypots.
The advantage of the test environment is that it is also suitable for developing machine learning models, malicious code, and exploits.

Keywords:

industrial cybersecurity, modbus TCP, MiTM, anomaly detection, machine learning

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VI.- Ipari kiberbiztonság Szekció

ZERO TRUST NETWORK ACCESS AZ IPARI KIBERBIZTONSÁGBAN - IPARI RENDSZEREK TÁVELÉRÉSÉNEK ÚJ MEGKÖZELÍTÉSE

TÓTH Ádám

A dolgozat az ipari irányítási rendszerek (OT) távelérésének kiberbiztonsági kihívásait vizsgálja, különös tekintettel a jelenleg elterjedt VPN-alapú megoldások sérülékenységeire, valamint a Zero Trust Network Access (ZTNA) technológia alkalmazási lehetőségeire. A jelenlegi megoldások támadási felületei rámutatnak a Zero trust elv szerint felépített, új típusú megoldások szükségességére. A ZTNA, a Tero trust architektúra elveire építve, finomhangolt, session-alapú hozzáférést, folyamatos kliensellenőrzést kínál. A dolgozat összeveti a ZTNA és VPN működését, bemutatja a ZTNA OT-ba történő integrációs lehetőségeit és kihívásait.

Kulcsszavak:

ipari rendszerek, OT, távoli elérés, ZTNA, zero-trust, zero-trust architektúra

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VI.- Operation Technology

ZERO TRUST NETWORK ACCESS SOLUTIONS IN OPERATIONAL TECHNOLOGY ENVIRONMENTS - NEW APPROACHES OF REMOTE ACCESS IN INDUSTRIAL ENVIRONMENTS

Ádám TÓTH

The thesis examines the cybersecurity challenges of remote access to industrial control systems (OT), with a particular focus on the vulnerabilities of currently widespread VPN-based solutions and the potential application of Zero Trust Network Access (ZTNA) technology. The attack surfaces of current solutions highlight the need for new approaches built on the Zero Trust principle. Based on the principles of Zero Trust Architecture, ZTNA offers fine-tuned, session-based access and continuous client verification. The thesis compares the operation of ZTNA and VPN, and presents the possibilities and challenges of integrating ZTNA into OT environments.

Keywords:

industrial control systems, OT, remote access, ZTNA, zero-trust, zero-trust architecture

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VI.- Ipari kiberbiztonság Szekció

SÉRÜLÉKENYSÉG ÉRTÉKELÉS ÉS SCORING RENDSZER KIALAKÍTÁS AZ OT SZEKTORBAN A CVE MÓDSZERTAN ALAPJÁN

NAGY Marcell

Az ipari irányítórendszerek (OT) kiberbiztonsági fenyegetettsége az elmúlt évtizedben drasztikusan megnőtt. Míg korábban az OT hálózatok szigetszerűen, az internettől elzártan működtek, mára egyre szorosabb integrációba kerültek az IT rendszerekkel és vállalatirányítási hálózatokkal. Ez a változás új támadási lehetőségeket teremtett, és olyan célzott kiberincidensek, mint a Stuxnet, a Triton vagy a NotPetya, már kifejezetten az ipari környezetek ellen irányultak. Az IT szektorban bevett sérülékenységértékelési módszerek – a CVE, a CVSS és az EPSS – önmagukban nem adnak megfelelő támpontot az OT világában, mivel nem tükrözik az üzembiztonság és a megbízhatóság elsődleges szerepét. A tanulmány részletesen bemutatja az IT és OT biztonsági megközelítések közötti különbségeket, majd ezek alapján egy új, OT-specifikus kockázatértékelési módszertant dolgoz ki. Az új modell a MITRE ATT&CK ICS mátrix támadási vektoraira, az EPSS valószínűségi mutatóira és hatásanalízisre épül, és Excel-alapú kalkulátorral teszi gyakorlati eszközzé a sérülékenységek értékelését. A módszertan célja, hogy a szervezetek hatékonyabban priorizálják a biztonsági intézkedéseket, növeljék a kritikus infrastruktúrák védelmét, valamint biztosítsák a NIS2 előírásainak való megfelelést.

Kulcsszavak:

OT biztonság, CVSS, EPSS, MITRE ATT&CK, kockázatértékelés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VI.- Operation Technology

VULNERABILITY ASSESSMENT AND SCORING SYSTEM DEVELOPMENT IN THE OT SECTOR BASED ON THE CVE METHODOLOGY

Marcell NAGY

The cybersecurity threats targeting Operational Technology (OT) systems have dramatically increased over the past decade. While OT networks traditionally operated in isolated environments, disconnected from the internet, today they are increasingly integrated with IT and enterprise management systems. This evolution has created new attack vectors, making OT infrastructures vulnerable to targeted incidents such as Stuxnet, Triton, or NotPetya. Conventional IT vulnerability assessment methods – including CVE, CVSS, and EPSS – are insufficient on their own in OT environments, as they fail to adequately address operational safety and system reliability. This study examines the key differences between IT and OT security approaches and introduces a tailored OT-specific risk assessment methodology. The proposed model builds on MITRE ATT&CK ICS attack vectors, EPSS probability scores, and impact analysis, while its implementation is supported by an Excel-based calculator that enables practical and accurate vulnerability evaluation. The methodology provides organizations with a more effective framework for prioritizing mitigation measures, strengthening the resilience of critical infrastructures, and ensuring compliance with the NIS2 directive.

Keywords:

OT security, CVSS, EPSS, MITRE attack, risk assessment

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VI.- Ipari kiberbiztonság Szekció

HOSSZÚ BÁJTOK ÉJSZAKÁJA AZ EESZT MŰKÖDTETŐJÉNÉL

ALEXIN Zoltán

Közérdekű adatkérés eredményeként került nyilvánosságra a kimittud.hu weboldalon, hogy 2022. első félévében jelentős mennyiségű személyes egészségügyi adatot adott át az EESZT működtetője két kutatócsoportnak. A Semmelweis Egyetem 3 millió COVID-19 oltásrekordot, 191 millió eKatalógus rekordot kapott EESZT rekordazonosítókkal, valamint 67 millió eReceptet TAJ azonosítóval. A Dél-Pesti Centrumkórház 69,5 millió PDF fájlt kapott személyes adatokkal. A Dél-Pesti Centrumkórház a kapott adatokat olyan MI algoritmus betanítására kívánta használni, amellyel a PDF formájú orvosi dokumentumok tartalmát számítógéppel elemezhető formájúra tudják alakítani. Az Adatvédelmi Hatóság saját hatáskörben hatósági eljárás megindításáról döntött, és annak végeztével a NAIH-4092-2/2024. iktatószámú határozatot bocsátotta ki. Azt állapította meg, hogy a Semmelweis Egyetem anonim adatokat dolgozott fel. A Dél-Pesti Centrumkórház számára a további kutatási tevékenységet az adatokon megtiltotta, és ennek következtében döntött úgy, hogy az érintetteket nem érte sérelem.
A szerző a fenti biztonsági eseményről megismerhető részleteket mutatja be a tanulságokkal és saját véleményének közreadásával.

Kulcsszavak:

EESZT, anonim adatok, mesterséges intelligencia, információs önrendelkezés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VI.- Operation Technology

NIGHT OF LONG BYTES AT THE MAINTAINER OF THE NATIONAL EHR SYSTEM

Zoltán ALEXIN

As a result of a freedom of information request it came to light on the kimittud.hu webpage, that in the first half of 2022, the maintainer of the national EHR system handed over a considerable amount of personal health data to two research groups. Semmelweis University received 3 million COVID-19 vaccination records and 191 million event catalog records, both with internal unique EHR identifiers, plus 67 million ePrescriptions with TAJ (Social Security Identifier). The South-Pest Hospital Centre received 69.5 million health document as PDF files with all natural personal identifiers. The South-Pest Hospital Centre intended to train an AI system by the received data in order to make such a system that is able transform a medical document in PDF into machine processable format. The Data Protection Authority decided to launch an ex officio procedure. At the end of its investigation, it issued the decision: NAIH-4092-2/2024. It found that the Semmelweis University processed anonymous data therefore no rights were violated. For the South-Pest Hospital Centre it prohibited further processing of data for research purposes, then concluded the no data subjects' rights were violated. The author would like to present the available details about this security event, the moral together with his own opinion.

Keywords:

national EHR system, anonymous data, artificial intelligence, informational self-determination

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VII.- Kiberbiztonság Szekció

Cybersecurity Session VII. - Cybersecurity

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VII.- Kiberbiztonság Szekció

A BITEK EGYÜTTÁLLÁSA

FICZERE Tamás

Az előadás témáját az élet hozta, mert a vizsgált esetettel havonta találkozunk a sérülékenység vizsgálatok során. Adott egy frissen tartott rendszer, melyet automata eszközökkel kívülről vizsgálva nem találunk sérülékenységet. A banner információkból megállapíthatjuk, hogy egy IIS 10 webszerver és egy Firebird adatbázis szolgáltatás fut a szerveren, mindkettő az aktuális, legfrissebb verzión. Ez az együttállás viszont a hozzáértő kezeknek egy kritikus sérülékenység jelenlétét feltételezi a rendszerben. Hogyan tudunk megbizonyosodni a sérülékenységről és hogyan tudjuk kihasználni?
Miért nem találta meg ezt az automata vizsgálati eszköz?

Kulcsszavak:

IIS10, FirebirdDatabase, asp, webshell, reverseshell

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VII.- Cybersecurity

WHEN THE BITS ALIGN

Tamás FICZERE

The topic of this presentation was inspired by real-life experience, as we encounter the examined case on a monthly basis during vulnerability assessments.

We are given a well-maintained system on which no vulnerabilities are detected through external automated scanning tools. Based on the banner information, we can identify that an IIS 10 web server and a Firebird database service are running on the server, both in their current, latest versions.

However, this combination suggests to knowledgeable hands that a critical vulnerability may be present in the system.

How can we verify the existence of this vulnerability and how can we exploit it?

Why was it not detected by the automated scanning tool?

Keywords:

IIS10, firebird database, asp, webshell, reverseshell

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VII.- Kiberbiztonság Szekció

MAGAS AUTOMATIZÁLTSÁGÚ KÖZÚTI KÖZLEKEDÉSI JÁRMŰVEK BALESETI ÉS EGYÉB FUNKCIONÁLIS ADATAINAK KINYERÉSE

RÉPÁS József

A ténylegesen önvezető módon közlekedő, magas automatizáltságú járművek széleskörű eltrjedésére még várni kell, azonban egyre inkább megjelennek a tesztpályán kívül is a fejlett vezetéstámogató rendszerrel rendelkező járművek. Ezen járművek a működésükhöz nagy mennyiségben gyűjtenek információt a környezetükről, a környező járművekről, a vezetőről. A gyűjtött adatok részben a jráművön belül, részben a járművön kívül, valamilyen felhő alapú rendszerben kerülnek tárolásra. Ez azt is jelenti, hogy a szakértői vizsgálatok során, lényegesen több elő és utómunkára van szükség, az adatok forrásának meghatrozásához, az adatokhoz való hozzáféréshez és a kinyeréshez. Az előzetes felkészülés során a vizsgált járműhöz kapcsolódóan szükségessé válhat a gyártói és hivatalos dokumentációk tanulámányozása mellett nyílt forrású információszerzés is, annak érdekében, hogy az adatokhoz való hozzáférés megvalósítható legyen. Mind az adatok vizsgálata, elemzése, mind értelmezése során szükséges lehet egyéb nem gyártói forrásból származó hivatalos információra is, hiszen a digitalizálódó járművek egyre inkább a kibertámadásokcélpontjává válnak, melyekről különböző fórumokon, a dark web-en további információ található meg.

Kulcsszavak:
modern járművek, szakértői vizsgálat, OSINT, jármű forensics

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VII.- Cybersecurity

EXTRACTION OF ACCIDENT AND OTHER FUNCTIONAL DATA OF HIGHLY AUTOMATED TRANSPORT VEHICLES

József RÉPÁS

The widespread use of highly automated vehicles that actually drive themselves has yet to be seen, but vehicles with advanced driver assistance systems are increasingly appearing outside the test track. These vehicles collect a large amount of information about their environment, the surrounding vehicles, and the driver in order to operate. The collected data is stored partly within the vehicle and partly outside the vehicle, in several cloud-based systems. This also means that during digital vehicle forensics examinations, significantly more pre- and post-work is required to determine the source of the data, access to the data, and extract it. During the preparation phase, in addition to studying the manufacturer and official documentation related to the vehicle, it may be necessary to obtain open-source information to access the data. During the examination, analysis, and interpretation of the data, it may be necessary to use official information from other non-manufacturer sources, as modern vehicles are increasingly becoming targets of cyberattacks, about which further information can be found on various forums and the dark web.

Keywords:
modern vehicles, digital forensics, OSINT, vehicle forensics

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VII.- Kiberbiztonság Szekció

IDŐZÁR-ALAPÚ KRIPTOGRÁFIAI MEGOLDÁS TENDEREK, KÖZBESZERZÉSEK ÉS ÁRAJÁNLATOKRA

NAGY Csaba Norbert, OLÁH Norbert

A digitális világ fejlődésével az adatok védelme és az információk szabályozott hozzáférése kiemelt biztonsági feladattá vált. Ahogy digitalizálódnak a rendszereink és egyre komplexebb adatvédelmi kihívások merülnek fel, úgy válik mindinkább szükségessé a megbízható, hatékony és sokoldalú titkosítási protokollok alkalmazása. Az időzített titkosítás a modern adatbiztonság egyik népszerű kutatási területe, amely garantálja, hogy az érzékeny információk kizárólag a kijelölt időpontban váljanak hozzáférhetővé. Célunk egy olyan hatékony időzített titkosítási protokoll megalkotása, amely biztosítja, hogy az adatok bizalmassága ne sérüljön több szereplő együttműködése esetén. A blokklánc technológia olyan keretrendszert biztosít az időzített titkosítás számára, amely a bizalmasság mellett integritásvédelmet, nyomonkövethetőséget és auditálhatóságot is garantál. A témában kétféle megoldást mutatunk be. Az első esetben a titkosító félnek egyértelmű érdeke fűződik az információ késleltetett hozzáférhetőségéhez. Második megoldásunk egy olyan kriptográfiai módszert javasol, amely lehetőséget biztosít a titkosított adatok utólagos módosítására Chameleon hash segítségével, amely a résztvevő felek közös megegyezésén alapul

Kulcsszavak:

Chameleon hash, időzár-alapú titkosítás, blokklánc, hyperledger fabric

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VII.- Cybersecurity

MODIFIABLE BLOCKCHAIN WITH TIME-LOCK ENCRYPTION PROTOCOL

Csaba Norbert NAGY, Norbert OLÁH

With the development of the digital world, data protection and controlled access to information have become key security tasks. As our systems become more digitalized and increasingly complex, data protection challenges arise, making the need for reliable, efficient, and versatile encryption protocols ever more pressing. Timed encryption is a popular area of research in modern data security, ensuring that sensitive information is only accessible at a designated time. Our goal is to create an effective timed encryption protocol that ensures data confidentiality is not compromised when multiple parties collaborate. Blockchain technology provides a framework for timed encryption that guarantees confidentiality, integrity protection, traceability, and auditability. We present two types of solutions in this area. In the first case, the encrypting party has a clear interest in delayed access to the information. Our second solution proposes a cryptographic method that allows for the subsequent modification of encrypted data using a Chameleon hash, which is based on the mutual agreement of the participating parties.

Keywords:

chameleon hash, time-lock encryption, blockchain, hyperledger fabric

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VII.- Kiberbiztonság Szekció

ADATHALÁSZAT HOME OFFICE-BÓL

SOLYMOS Ákos

Az előadás az adathalászat (phishing) 2005 és 2025 közötti fejlődését vizsgálja, különös tekintettel a magyarországi pénzintézeti támadások történetére és a kiberbűnözés társadalmi hátterére. Áttekintem az első hazai banki adathalászatok jellegzetességeit, majd bemutatom, miként változtak az adathalász üzenetek, hamis weboldalak és csatornák — az e-mailes csalásoktól a közösségi médiás és telefonos adathalászatokig. Bemutatásra kerül egy valós, hibásan megírt adathalász weboldal, amelyen keresztül betekintést nyerhetünk a színfalak mögé. Az előadás záró akkordjaként saját scam baiting tevékenységem eredményeként két valós, megélhetési kiberbűnözőkkel folytatott beszélgetést ismertetek, amelyek betekintést nyújtanak abba, hogyan működik a kiberbűnözés ökoszisztémája.

Kulcsszavak:

adathalászat, kiberbűnözés, scam baiting, digitális bűnözés ökoszisztéma, információvédelem

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VII.- Cybersecurity

HOME-BASED PHISHING ATTACKS

Ákos SOLYMOS

The presentation examines the evolution of phishing between 2005 and 2025, with a particular focus on the history of phishing attacks targeting Hungarian financial institutions and the social background of cybercrime. It reviews the characteristics of the earliest Hungarian banking phishing incidents and traces the transformation of phishing messages, fraudulent websites, and attack channels—from early e-mail scams to social media and phone-based phishing schemes. A real, poorly coded phishing website will be analyzed, offering a glimpse behind the scenes of such operations. As the concluding highlight, I will present two authentic conversations recorded during my own scam-baiting activities, providing insight into the functioning of the cybercrime ecosystem and the mindset of profit-driven, livelihood-oriented cyber offenders.

Keywords:

phishing, cybercrime, scam baiting, cybercrime ecosystem, information security

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VII.- Kiberbiztonság Szekció

VEZETŐI KOMPETENCIÁK ÉS NEMI KÜLÖNBSÉGEK A KIBERBIZTONSÁG TERÜLETÉN MAGYARORSZÁGON: A NŐI VEZETŐK ELŐTT ÁLLÓ KIHÍVÁSOK ÉS ELŐMENETELI LEHETŐSÉGEK ELEMZÉSE

GALBÁCS Erika

Jelen kutatás a női vezetők érvényesülési lehetőségeit és a nemi sajátosságokból fakadó strukturális akadályokat vizsgálja a kiberbiztonság területén, feltérképezve, milyen tényezők segítik vagy hátráltatják előmenetelüket ezen a technikailag intenzív, hagyományosan férfiak által dominált szakterületen. A tanulmány kvalitatív és kvantitatív módszereket alkalmazott: egy 25 kérdéses kérdőív és három mélyinterjú szolgáltatta az empirikus alapot. A kvantitatív adatok szerint a mentorálás és a hálózatépítés hiánya jelentős karrierakadály, míg a mélyinterjúk rávilágítottak a nemi sztereotípiák és a „token" jelenlét pszichológiai terheire – például a folyamatos bizonyítási kényszerre vagy a kompetencia megkérdőjelezésére –, amelyek főként felsővezetői szinteken erősek. Pozitív példaként említhetők a bankszektor junior és senior tehetséggondozó programjai, amelyek célzott támogatást nyújtanak a női szakembereknek. Az eredmények hozzájárulnak a nemi egyenlőtlenségek jobb megértéséhez, és kiemelik a strukturált mentorálás, a támogató hálózatok és a szervezeti kultúraváltás kulcsszerepét a női vezetők előmenetelében.

Kulcsszavak:

kiberbiztonság, női vezetők, nemi sztereotípiák, mentorálás, hálózatépítés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VII.- Cybersecurity

LEADERSHIP COMPETENCIES AND GENDER DIFFERENCES IN THE FIELD OF CYBERSECURITY IN HUNGARY: AN ANALYSIS OF THE CHALLENGES AND CAREER ADVANCEMENT OPPORTUNITIES FOR WOMEN LEADERS

Erika GALBÁCS

This study examines the career advancement opportunities of women leaders and the structural barriers arising from gender-specific factors in the field of cybersecurity, mapping out the elements that either facilitate or hinder their progress in this technically intensive, traditionally male-dominated domain. The research employed both qualitative and quantitative methods: a 25-question survey and three in-depth interviews served as the empirical foundation. Quantitative data indicate that the lack of mentoring and networking poses a significant career obstacle, while the interviews highlighted the psychological burdens of gender stereotypes and "token" presence—such as the constant need to prove oneself or the questioning of professional competence—which are particularly prevalent at senior leadership levels. As positive examples, the study cites junior and senior talent development programs in the banking sector, which provide targeted support for female professionals. The findings contribute to a better understanding of gender inequalities in cybersecurity and emphasize the key role of structured mentoring, supportive professional networks, and organizational cultural change in advancing women leaders.

Keywords:

cybersecurity, women leaders, gender stereotypes, mentoring, networking

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VIII. - Kutatás, fejlesztés III. szekció

Cybersecurity - Session VIII. - Research and Development III.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VIII. - Kutatás, fejlesztés III. szekció

KÖZLEKEDÉS IRÁNYÍTÁSI ESZKÖZÖK A NIS2 TÜKRÉBEN

KATONA Gergő

Az intelligens közlekedési irányítási rendszerek az Európai Unió kritikus közlekedési ágazatához tartoznak, így működésük során elengedhetetlen a kiberbiztonsági megfelelés a NIS2 irányelv előírásainak. A NIS2 azonban csupán általános követelményrendszert határoz meg, a részletes szabályozás tagállami szinten valósul meg, ami jelentős eltéréseket eredményez az egyes országok megközelítéseiben. A kutatás célja ezen nemzeti szintű különbségek azonosítása és rendszerezése az intelligens közlekedési irányítási eszközök információbiztonsági szabályozása terén. Az elemzés feltárja a harmonizáció hiányából fakadó kockázatokat, valamint megvizsgálja, hogy a különböző tagállami megoldások milyen mértékben járulnak hozzá, vagy épp gátolják egy egységes, uniós szintű biztonsági architektúra kialakítását. Az eredmények hozzájárulhatnak egy olyan átfogó, közös biztonsági keretrendszer megalapozásához, amely a NIS2 irányelv célkitűzéseit minden tagállamban egységesen, mégis rugalmasan képes érvényesíteni, elősegítve az EU-szintű közlekedési irányítás biztonságos integrációját.

Kulcsszavak:

NIS2, közúti közlekedés, kiberbiztonság, kritikus infrastruktúra

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VIII. - Research and Development III.

TRANSPORT MANAGEMENT SYSTEMS IN THE CONTEXT OF NIS2

Gergő KATONA

Intelligent traffic management systems belong to the European Union's critical transport sector, making compliance with the NIS2 Directive's cybersecurity requirements essential. However, NIS2 provides only a general regulatory framework, while the detailed provisions are defined at the national level, leading to significant divergences among Member States. The aim of this research is to identify and categorize these national-level differences in the cybersecurity regulation of intelligent traffic management tools. The analysis highlights the risks arising from the lack of harmonization and examines how different national approaches either contribute to or hinder the development of a unified EU-wide security architecture. The findings support the foundation of a comprehensive and harmonized security framework that can apply the objectives of the NIS2 Directive consistently across all Member States, while maintaining sufficient flexibility to adapt to local contexts, thereby facilitating the secure integration of EU-level traffic management systems.

Keywords:

NIS2, road transportation, cybersecurity, critical infrastructure

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VIII.- Kutatás, fejlesztés III.Szekció

A DIGITÁLIS TÉR, MINT ÚJ KOCKÁZATI KÖRNYEZET: KULTURÁLIS JAVAK A DARK WEB ÁRNYÉKÁBAN

HORVÁTH Illés

Az utóbbi években a műkincsek és régészeti leletek illegális kereskedelme új színtérre helyeződött át: a dark web hálózataira és a blokklánc-alapú tranzakciós rendszerekre. Míg korábban a feketepiac hagyományos csatornái domináltak, ma már egyre több bizonyíték támasztja alá, hogy a kulturális javak kereskedelme rejtett online piactereken is jelen van. A folyamatot tovább erősíti a kriptovaluták és az NFT-k elterjedése, amelyek új értékátviteli és álcázási mechanizmusokat kínálnak az elkövetők számára. Előadásomban a jelenség operatív és technológiai dimenzióit kívánom bemutatni – a Tor-hálózat által biztosított anonimitástól a virtuális eszközökkel végrehajtott értéktranszferekig – és rámutatok arra, hogy már az Europol és Interpol által koordinált Pandora-műveletek során is azonosítottak olyan digitális nyomokat, amelyek a kulturális javak dark webes kereskedelmére utaltak. Előadásommal arra kívánom felhívni a figyelmet, hogy a régiségek illegális piacának digitális formája már nem marginális, hanem egyre inkább terjedő, a kiberbűnözés ökoszisztémájába szervesen beépülő jelenség.

Kulcsszavak:

dark web, kulturális javak, blokklánc-alapú tranzakciók, kriptovaluták, NFT-k

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VIII. - Research and Development III.

THE DIGITAL SPACE AS A NEW RISK ENVIRONMENT: CULTURAL PROPERTIES IN THE SHADOW OF THE DARK WEB

Illés HORVÁTH

In recent years, the illegal trafficking of cultural properties and archaeological artefacts has moved to a new arena: dark web networks and blockchain-based transaction systems. While traditional black market channels used to dominate, there is now growing evidence that cultural property is also being traded on hidden online marketplaces. This process is further reinforced by the spread of cryptocurrencies and NFTs, which offer new value transfer and concealment mechanisms for perpetrators. In my presentation, I will outline the operational and technological dimensions of this phenomenon – from the anonymity provided by the Tor network to value transfers carried out with virtual assets – and point out that digital traces indicating the dark web trade in Cultural Properties have already been identified during the Pandora operations coordinated by Europol and Interpol. With my presentation, I wish to draw attention to the fact that the digital form of the black market in antiquities is no longer a marginal phenomenon, but one that is becoming increasingly widespread and is becoming an integral part of the cybercrime ecosystem.

Keywords:

dark web, cultural assets, blockchain-based transactions, cryptocurrencies, NFTs

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VIII.- Kutatás, fejlesztés III.Szekció

NEM CSAK A GÉP HIBÁZIK, A FELELŐSSÉG HÁZON BELÜL KEZDŐDIK

KISS Tamás

A komplex informatikai rendszerek fejlesztése és üzemeltetése során gyakran az a téves feltételezés él, hogy a biztonsági és működési problémák elsődlegesen technológiai eredetűek. A tapasztalat azonban azt mutatja, hogy az incidensek, sérülékenységek és működési zavarok jelentős része szervezeti és felelősségi hiányosságokra vezethető vissza. A „nem az én dolgom” szemlélet, az egymásra mutogatás, valamint a döntési és jóváhagyási jogkörök tisztázatlansága komoly kockázatot jelent a fejlesztési életciklus minden szakaszában. Különösen igaz ez akkor, amikor több szervezeti egység, külső beszállító és eltérő szakmai terület vesz részt egy rendszer megvalósításában. A fejlesztési folyamatok során ezért nem elegendő kizárólag a technikai követelmények, funkciók és biztonsági kontrollok meghatározása. Legalább ilyen fontos annak egyértelmű rögzítése, hogy az egyes feladatokért, döntésekért és kockázatokért ki viseli a felelősséget. A felelősségek tisztázatlansága nemcsak a hibák elhárítását nehezíti meg, hanem akadályozza a hatékony kommunikációt, lassítja a döntéshozatalt, és növeli a szervezeti kockázatokat is. E problémák kezelésére az egyik legátláthatóbb és leginkább bevált módszer a RACI mátrix alkalmazása. A felelősség nem ruházható át eseti jelleggel vagy utólag: annak már a rendszer tervezési és fejlesztési szakaszában egyértelműen meghatározottnak kell lennie.

Kulcsszavak:

szervezeti felelősség, RACI matrix, kockázatcsökkentés, fejlesztési életciklus, biztonságtudatos működés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VIII. - Research and Development III.

IT'S NOT ONLY THE MACHINE THAT FAILS: RESPONSIBILITY BEGINS WITHIN THE ORGANISATION

Tamás KISS

During the development and operation of complex information systems, there is often a mistaken assumption that security and operational issues are primarily technological in nature. Experience shows, however, that a significant proportion of incidents, vulnerabilities, and operational disruptions stem from organisational shortcomings and unclear responsibilities. The "not my task" attitude, mutual blame-shifting, and the lack of clearly defined decision-making and approval authorities pose substantial risks throughout the entire system development lifecycle, especially when multiple organisational units, external suppliers, and diverse professional domains are involved. In such environments, it is not sufficient to define only technical requirements, functionalities, and security controls. It is equally important to clearly assign responsibility for tasks, decisions, and risk ownership. Unclear accountability not only complicates incident resolution but also hinders effective communication, slows decision-making processes, and increases organisational risk. One of the most transparent and widely adopted methods for addressing these challenges is the application of the RACI matrix. Responsibility cannot be assigned retroactively; it must be clearly defined from the earliest stages of system design and development.

Keywords:

organisational responsibility, RACI matrix, risk mitigation, system development lifecycle, security-conscious operation

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VIII.- Kutatás, fejlesztés III.Szekció

FELSŐOKTATÁSI HALLGATÓK BIZTONSÁGTUDATOSSÁGA A SAM MODELL ALAPJÁN

VINOGRADOV Sergey, BEREK László, OLÁH Norbert,
UJHEGYI Péter, RÉPÁS József, LASKA Pál

A felhasználók biztonságtudatosságának mérése ezért kulcsfontosságú a hatékony védelem és a célzott oktatási programok kialakítása szempontjából. Jelen kutatás a Security Awareness Model (SAM) bemutatására és empirikus tesztelésére vállalkozik, amely a korábbi HAIS-Q modellt továbbfejlesztve a Tudás–Attitűd–Viselkedés dimenziókat tíz szakmai terület mentén – többek között jelszóhasználat, webes biztonság, személyes adatok védelme vagy incidensmenedzsment – integrálja. A pilotkutatás 132 felsőoktatási hallgató válaszain alapult, és célja a modell konstrukcióinak megbízhatósági és érvényességi vizsgálata volt. Az eredmények alapján mindhárom komponens dimenziói szignifikánsan hozzájárulnak az általános biztonsági tudáshoz, ugyanakkor néhány tétel újrafogalmazása indokolt a mérési pontosság javítása érdekében. A hallgatók legnagyobb egyetértést a klasszikus biztonsági kockázatok (pl. ismeretlen USB-eszközök, adathalászat) terén mutatták, míg a szabályozási tudatosság és az új technológiákhoz kapcsolódó attitűdök esetében jelentős bizonytalanság tapasztalható. A SAM modell alkalmas az információbiztonsági tudatosság komplex, többdimenziós feltárására, és alapot nyújt nagymintás, országos vizsgálatokhoz, amelyek hozzájárulhatnak a biztonsági kultúra fejlesztéséhez a felsőoktatásban és a társadalom szélesebb körében.

Kulcsszavak:

információbiztonság, biztonságtudatosság, SAM modell, HAIS-Q, felsőoktatás, pilotkutatás

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VIII. - Research and Development III.

SECURITY AWARENESS AMONG HIGHER EDUCATION STUDENTS BASED ON THE SAM MODEL

Sergey VINOGRADOV, László BEREK,
Norbert OLÁH, Péter UJHEGYI, József RÉPÁS,
Pál Károly LASKA

Measuring users' security awareness is crucial for adequate protection and developing targeted education programs. This research aims to present and empirically test the Security Awareness Model (SAM), which builds on the previous HAIS-Q model by integrating the Knowledge-Attitude-Behaviour dimensions across ten professional areas, including password use, web security, personal data protection, and incident management. The pilot study was based on the responses of 132 higher education students and aimed to test the reliability and validity of the model's constructs. Based on the results, all three component dimensions contribute significantly to general security knowledge, but some items need to be reworded to improve measurement accuracy. The students agreed on classic security risks (e.g., unknown USB devices, phishing). At the same time, there was significant uncertainty in regulatory awareness and attitudes toward new technologies. The SAM model is suitable for the complex, multidimensional exploration of information security awareness and provides a basis for large-scale, nationwide studies that can contribute to developing a security culture in higher education and society.

Keywords:

information security, security awareness, SAM model, HAIS-Q, pilot research, higher education

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság VIII.- Kutatás, fejlesztés III.Szekció

BLOKKLÁNC-ALAPÚ ELSZÁMOLÁSI RENDSZER A KÖNYVIPARBAN

OLÁH Norbert, NAGY Csaba Norbert

A könyvtári és kiadói ökoszisztéma működése napjainkban egyre inkább az adatvezérelt döntéshozatalra és az információáramlás hatékony menedzsmentjére épül. A könyvtárak és kiadók számára a felhasználói viselkedésről származó adatok – például a kölcsönzési szokások, a vásárlási trendek, a legnépszerűbb műfajok és szerzők, valamint a felhasználói demográfiai jellemzők – közvetlenül hozzájárulnak a szolgáltatások optimalizálásához (például a keresett könyvek beszerzéséhez és a készletgazdálkodás javításához), a felhasználói igények előrejelzéséhez (például egyes műfajok iránti növekvő érdeklődés azonosításához), valamint a stratégiai tervezéshez (például célzott kiadói kampányok vagy könyvtári programok kialakításához).
A tanulmány egy olyan blokklánc-alapú elszámolási rendszer megtervezését célozza, amely lehetővé teszi a felhasználói adatokból képzett aggregált statisztikai információk biztonságos, átlátható és adatvédelmi szempontból megfelelő hasznosítását a kiadói és könyvtári döntéshozatal támogatására. A javasolt rendszer konzorciumi blokklánc-architektúrán alapul, amely ötvözi a blokklánc-technológia olyan előnyeit, mint az adatok módosíthatatlansága, auditálhatósága a korlátozott hozzáférésű és bizalmas adatkezelés lehetőségével. A Private Data Collection mechanizmus révén az érzékeny adatok kizárólag az arra jogosult szereplők között oszthatók meg, miközben azok integritása a teljes hálózat által garantált.

Kulcsszavak:

fair elszámolási rendszer, blokklánc, hyperledger fabric, kriptográfia

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session VIII. - Research and Development III.

BLOCKCHAIN-BASED ACCOUNTING SYSTEM IN THE BOOK INDUSTRY

Norbert OLÁH, Csaba Norbert NAGY

The operation of the library and publishing ecosystem today increasingly relies on data-driven decision-making and the effective management of information flows. For libraries and publishers, data derived from user behavior—such as borrowing habits, purchasing trends, the most popular genres and authors, as well as user demographic characteristics—directly contribute to service optimization (e.g., acquiring in-demand books and improving inventory management), forecasting user needs (e.g., identifying the growing interest in certain genres), and strategic planning (e.g., developing targeted publishing campaigns or library programs). This study aims to design a blockchain-based settlement system that enables the secure, transparent, and privacy-compliant utilization of aggregated statistical information derived from user data to support decision-making in publishing and library operations. The proposed system is based on a consortium blockchain architecture, which combines the advantages of blockchain technology—such as data immutability and auditability—with the ability to manage confidential data under restricted access. Through the Private Data Collection mechanism, sensitive data can be shared exclusively among authorized participants, while their integrity remains guaranteed by the entire network.

Keywords:

fair settlement system, blockchain, hyperledger fabric, cryptography

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IX.- NIS2 Szekció

Cybersecurity Session IX.- NIS2

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IX.- NIS2 Szekció

A HAZUGSÁG ANATÓMIÁJA: AZ ÁLHÍREK PSZICHOLÓGIÁJA ÉS DRAMATURGIÁJA

LASKA Pál Károly

A dezinformációs kutatás a Nemzeti Közszolgálati Egyetem hallgatói körében zajlott, és azt vizsgálta, hogyan épülnek fel az álhírek narratívái, valamint miként hatnak az érzelmek és a történetmesélés a befogadói döntéshozatalra. A hallgatók csoportmunkában szimulálták különböző célcsoportok – fiatalok, idősek, kormányzati szervezetek, vállalkozások és média/influenszerek – befolyásolását, egy-egy fiktív álhír forgatókönyvének megalkotásával.

A kutatás fő célja az volt, hogy feltárja, miként működik a pszichológiai hadviselés civil környezetben, és hogyan alkalmazzák a történetmesélés eszközeit a manipulációban: karakterépítés, konfliktus, érzelmi azonosulás és bizalomépítés. Az eredmények rávilágítottak arra, hogy a dezinformáció nem csupán technológiai, hanem kulturális és dramaturgiai jelenség is, amely a közönség érzelmi igényeire és világmagyarázati vágyára épít. A kutatás tapasztalatai alapján a tudatosítás és az oktatás egyik leghatékonyabb módja az, ha a hallgatók nemcsak felismerni, hanem megérteni tanulják meg a manipuláció narratív struktúráit – így válva ellenállóbbá az információs háború új formáival szemben.

Kulcsszavak:

álhírek, történetmesélés, dezinformáció, pszichológiai hadviselés, manipulációs narratívák

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session IX. - NIS2

THE SCRIPT OF DECEPTION: HOW FAKE NEWS NARRATIVES MANIPULATE EMOTIONS AND TRUST

Pál Károly LASKA

This research was conducted within the framework of the National University of Public Service (NUPS) course, exploring how misinformation narratives are constructed and how storytelling techniques influence emotional and cognitive responses. Students worked in groups to simulate the manipulation of different target audiences — including young people, elderly citizens, governmental institutions, businesses, and media influencers — by developing fictional disinformation scripts.
The study aimed to reveal how psychological warfare operates in civil information spaces and how narrative tools such as character building, emotional engagement, and conflict resolution are used to enhance persuasive impact. Findings indicate that disinformation is not only a technological issue but also a cultural and dramaturgical phenomenon, exploiting the audience's emotional needs and desire for coherent explanations.
The pedagogical approach demonstrates that awareness programs are more effective when participants do not only detect but also understand the underlying narrative structures of manipulation, thereby strengthening their resilience against contemporary forms of information warfare.

Keywords:

fake news, storytelling, disinformation, psychological warfare, manipulative narratives

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IX.- NIS2 Szekció

AZ ELSŐ KIBERBIZTONSÁGI AUDITOK TAPASZTALATAI – KIHÍVÁSOK ÉS TANULSÁGOK A GYAKORLATBAN

ACSAI Tamás

A 2024. évi LXIX. törvény a NIS2 irányelv hazai adaptációjaként új szintre emeli a kiberbiztonsági megfelelés követelményeit, ugyanakkor alkalmazása során számos értelmezési és végrehajtási nehézség merül fel. Előadásomban az eddig végrehajtott kiberbiztonsági auditok tapasztalatait alapul véve mutatom be legújabb kutatási tervemet, amelynek célja az első auditok tapasztalatainak feltárása az auditorok szemszögéből. A jelenlegi gyakorlat azt mutatja, hogy a szervezetek többsége teljesítette az előírt megfelelési szinteket, ugyanakkor egyre több olyan strukturális és értelmezési probléma kerül felszínre, amelyek érdemben befolyásolják az auditok hatékonyságát és eredményét. Fontos szerepet játszanak az előzetesen alkalmazott információbiztonsági szabványok és keretrendszerek, amelyek – bár önmagukban nem elegendőek a megfeleléshez – érezhetően támogatják a felkészülést. A kutatás várható eredményei rámutathatnak arra, hogy a heterogén érintetti kör és a jogszabályi környezet értelmezésének bizonytalanságai részletesebb iránymutatásokat igényelnek. Emellett felmerülhet az az igény is, hogy a megfelelési követelmények, az erőforrás-befektetés és az auditálás költségei között fenntartható egyensúlyt kell kialakítani úgy, hogy a NIS2 irányelv célja – a magasabb szintű kiberbiztonság – továbbra is megvalósulhasson.

Kulcsszavak:

NIS2 irányelv, kiberbiztonsági megfelelés, kiberbiztonsági audit, információbiztonsági szabványok

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session IX. - NIS2

EXPERIENCES FROM THE FIRST CYBERSECURITY AUDITS – CHALLENGES AND LESSONS FROM PRACTICE

Tamás ACSAI

Act LXIX of 2024, adopted as the national implementation of the NIS2 Directive, significantly raises the requirements for cybersecurity compliance in Hungary. However, its practical application has revealed numerous interpretative and implementation challenges. In my presentation, I will introduce my latest research plan, based on the experiences of the first cybersecurity audits, aiming to explore these audits from the perspective of auditors. Current practice shows that most organizations have met the required compliance levels; however, an increasing number of structural and interpretative issues are emerging that substantially affect the effectiveness and outcomes of the audits. Pre-existing information security standards and frameworks play an important role in preparation, as they offer clear advantages—although they are not sufficient on their own to ensure compliance. The expected results of the research may highlight the need for more detailed guidance, due to the heterogeneity of affected entities and the uncertainties in interpreting legal requirements. Furthermore, it may also emphasize the importance of establishing a sustainable balance between compliance expectations, resource investments, and audit costs, in a way that ensures the NIS2 Directive's ultimate goal—achieving a higher level of cybersecurity—remains attainable.

Keywords:

NIS2 Directive, cybersecurity compliance, cybersecurity audit, information security standards

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság IX.- NIS2 Szekció

A NIS2 MEGFELELÉS HUMÁN KOCKÁZATI VONATKOZÁSAI

NAGY István

A NIS2 megfelelés kapcsán a munkáltatónak vizsgálnia és szabályoznia kell a humán megfelelés és alkalmazás kockázatait. Az auditra való felkészülés kapcsán az alkalmazás jogi megfelelése mellett a NIS2 kiberbiztonsági megfelelését is vizsgálni szükséges. A vizsgálat feltételeit a 7/2024 MK rendelet Személyi biztonság fejezet tartalmazza, ami részletesen tárgyalásra került.
Áttekintésre kerülnek az előadás során a NIST SP 800-53 PS: Personal Security szabvány munkavállalókat érintő részletei.

Kulcsszavak:

humánkockázat, NIS2, ISO 27001, NIST

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session IX. - NIS2

HUMAN RISK ASPECTS OF NIS2 COMPLIANCE

István NAGY

In the context of NIS2 compliance, employers are required to assess and regulate the risks related to human compliance and the secure use of applications by employees. When preparing for an audit, it is necessary to examine not only the legal compliance of an application, but also its compliance with NIS2 cybersecurity requirements. The conditions and requirements of such assessments are defined in the Personal Security chapter of Government Decree 7/2024, which is discussed in detail in the presentation. Furthermore, the presentation provides an overview of the employee-related provisions of the NIST SP 800-53 PS (Personnel Security) standard.

Keywords:

human risk, NIS2, ISO 27001, NIST

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság X.- Kutatás, fejlesztés IV.Szekció

Cybersecurity Session X.- Research and Development IV.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság X.- Kutatás, fejlesztés IV.Szekció

AI ÉS BLOKKLÁNC INTEGRÁCIÓJA A KIBERBIZTONSÁGI SÉRÜLÉKENYSÉGEK AUTOMATIZÁLT ELEMZÉSÉRE

SZABÓ Sándor, OLÁH Norbert

A kutatás egy olyan biztonságtechnikai architektúrát mutat be, amely megoldást kínál a sérülékenységek feldolgozására és értékelésére. A rendszer az OWASP ZAP, az SQLmap és a Nessus eszközök kimeneteit egységes JSON formátumban dolgozza fel, ezzel elősegítve az átlátható adatkezelést, a strukturált feldolgozást és az elemzések hatékonyságát. Az architektúra egyik központi eleme a mesterséges intelligencia-modul, amely két különböző nyelvi modell API-integrációjára épül. Az AI három fő funkciót lát el: összefoglalja a sérülékenységekkel kapcsolatos információkat, kockázatbesorolást készít a CVSS és STRIDE modellek alapján, valamint konkrét javítási javaslatokat fogalmaz meg. Ezáltal a rendszer képes a nagy mennyiségű adat automatikus elemzésére, és segíti a szakembereket abban, hogy gyorsabban reagáljanak a potenciális biztonsági problémákra. Az adatok hitelességét és változatlanságát a Hyperledger Fabric blokklánc és az IPFS (InterPlanetary File System) integrációja garantálja. Az IPFS a nagyméretű adatok decentralizált tárolását biztosítja, míg a blokkláncon csak a tartalomazonosító (CID) és a sérülékenység-azonosító kerül rögzítésre. Ez a megoldás biztosítja az adatok integritását, visszakövethetőségét és a manipuláció kizárását. A bemutatott architektúra újdonsága abban rejlik, hogy egységes keretben integrálja a sérülékenységvizsgálat, az adatfeldolgozás, a mesterséges intelligencia és a blokklánc-technológia elemeit.

Kulcsszavak:

kiberbiztonság, AI, blokklánc, IPFS, sérülékenységkezelés

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session X. - Research and Development IV.

INTEGRATION OF AI AND BLOCKCHAIN IN THE AUTOMATED ANALYSIS OF CYBERSECURITY VULNERABILITIES

Sándor SZABÓ, Norbert OLÁH

This study presents a security architecture that automates the processing and evaluation of vulnerabilities. The system integrates outputs from OWASP ZAP, SQLmap, and Nessus into a unified JSON format, ensuring transparent data management and efficient analysis. A key component is the artificial intelligence module, built on the API integration of two language models. It summarizes vulnerability information, performs risk classification using CVSS and STRIDE models, and generates remediation recommendations. The system automates large-scale data analysis while maintaining human oversight, combining the efficiency of AI with expert reliability and reducing manual workload. Data authenticity and immutability are ensured through the integration of Hyperledger Fabric blockchain and IPFS (InterPlanetary File System). IPFS enables decentralized storage of large datasets, while only the content identifier (CID) and vulnerability ID are recorded on the blockchain. The proposed architecture unifies vulnerability assessment, data processing, artificial intelligence, and blockchain in a single auditable framework.

Keywords:

cybersecurity, AI, blockchain, IPFS, vulnerability management

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság X.- Kutatás, fejlesztés IV.Szekció

DECENTRALIZÁLT, NFC-ALAPÚ HITELESÍTÉSI PROTOKOLL SZIMMETRIKUS KRIPTOGRÁFIÁVAL ÉS ELOSZTOTT KULCSKEZELÉSSEL

PANKOTAI Imre, OLÁH Norbert

A modern digitális gazdaságban a központosított hitelesítési rendszerek komoly biztonsági kockázatot jelentenek, mivel az egyetlen hibapont miatt a teljes adatbázis veszélybe kerülhet kompromitálódás esetén. Ezen problémára válaszul a kutatás célja egy olyan decentralizált, NFC-alapú hitelesítési protokoll kidolgozása, amely a termékek eredetiségének igazolását és a tulajdonosi lánc biztonságos nyomon követését valósítja meg kizárólag szimmetrikus kriptográfia, konkrétan AES-algoritmus alkalmazásával. A rendszer a sebezhető központi hitelesítést egy elosztott, konzorcium-alapú modellre cseréli, ahol minden egyes NFC eszköz egyedi AES kulcsát egy Shamir-féle titokmegosztási eljárással titokrészekre bontják, és ezeket a hitelesítő csomópontok között osztják szét. A hitelesítési folyamat a közös AES kulcson alapul, ahol az NFC eszköz által küldött titkosított üzenetet a csomópontok egy biztonságos többpárti számítás (MPC) protokoll keretében együttesen fejtenek vissza anélkül, hogy a teljes AES kulcsot rekonstruálnák vagy egymásnak felfednék a kulcsrészeiket. A közös munka helyességét és naplózását egy konzorciumi blokklánc segítségével ellenőrizhetjük, amely egy megváltoztathatatlan és auditálható naplót biztosít minden hitelesítési eseményről, garantálva ezzel az eljárás ellenállóságát a visszajátszásos és klónozási támadásokkal szemben.

Kulcsszavak:

NFC, AES, Shamir-féle titokmegosztás, MPC, blokklánc

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session X. - Research and Development IV.

DECENTRALIZED NFC-BASED AUTHENTICATION PROTOCOL WITH SYMMETRIC CRYPTOGRAPHY AND DISTRIBUTED KEY MANAGEMENT

Imre PANKOTAI, Norbert OLÁH

In the modern digital economy, centralized authentication systems pose a serious security risk, as a single point of failure can compromise the entire database in the event of a breach. In response to this problem, the aim of the research is to develop a decentralized, NFC-based authentication protocol that verifies the authenticity of products and securely tracks the chain of ownership using only symmetric cryptography, specifically the AES algorithm. The system replaces vulnerable central authentication with a distributed, consortium-based model, where each NFC device's unique AES key is split into secret shares using a Shamir secret sharing scheme and distributed among the authentication nodes. The authentication process is based on a shared AES key, where the encrypted message sent by the NFC device is jointly decrypted by the nodes using a secure multi-party computation (SMPC) protocol without reconstructing the entire AES key or revealing their key shares to each other. The correctness and logging of the joint work can be verified using a consortium blockchain, which provides an immutable and auditable log of all authentication events, thus guaranteeing the resistance of the procedure to replay and cloning attacks.

Keywords:

NFC, AES, Shamir's Secret Sharing, MPC, blockchain

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kiberbiztonság X.- Kutatás, fejlesztés IV.Szekció

AI GENERÁLT TARTALMAK ÉS AZOK DETEKTÁLÁSA A FELSŐOKTATÁSBAN

BEREK László

A mesterséges intelligencia (MI) alapú szöveggeneráló eszközök gyors és széles körű elterjedése alapvetően alakítja át a felsőoktatás oktatási, tanulási és értékelési folyamatait. A nagy nyelvi modellekre épülő alkalmazások új lehetőségeket kínálnak a tanulás támogatására, ugyanakkor komoly kihívásokat jelentenek az akadémiai integritás, az értékelés megbízhatósága és a hallgatói teljesítmények eredetiségének ellenőrzése szempontjából. Az előadás célja, hogy átfogó képet nyújtson az MI-generált szövegek felsőoktatási megjelenéséről, valamint bemutassa az ezek felismerésére alkalmazott jelenlegi detektálási módszereket és eszközöket.

Az előadás első része röviden áttekinti az MI-alapú szöveggenerálás technológiai hátterét és tipikus felhasználási módjait a felsőoktatásban, különös tekintettel az írásbeli feladatokra, beadandókra és vizsgákra. Ezt követően az előadás elemzi a leggyakrabban alkalmazott detektálási megközelítéseket, beleértve a statisztikai, nyelvészeti és mesterséges intelligencián alapuló felismerési modelleket.

Az előadás záró részében javaslatokat fogalmaz meg arra vonatkozóan, hogyan integrálható az MI-tudatosság az oktatási gyakorlatba, milyen irányelvek mentén alakíthatók ki átlátható és fenntartható intézményi szabályozások, valamint miként támogatható az MI felelős és transzparens használata a felsőoktatásban.

Kulcsszavak:

mesterséges intelligencia, MI-generált tartalmak, szöveggenerálás, felsőoktatás, akadémiai integritás, tartalomdetektálás

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Cybersecurity Session X. - Research and Development IV.

AI-GENERATED CONTENT AND ITS DETECTION IN HIGHER EDUCATION

László BEREK

The rapid and widespread adoption of artificial intelligence based text generation tools is fundamentally transforming teaching, learning, and assessment processes in higher education. Applications built on large language models offer new opportunities to support learning; at the same time, they pose significant challenges to academic integrity, the reliability of assessment, and the verification of the originality of student work. The aim of this presentation is to provide a comprehensive overview of the emergence of AI-generated texts in higher education and to introduce the currently applied methods and tools for their detection.

The first part of the presentation briefly outlines the technological background of AI-based text generation and its typical use cases in higher education, with a particular focus on written assignments, coursework, and examinations. This is followed by an analysis of the most commonly used detection approaches, including statistical, linguistic, and AI-based recognition models.

In the final part of the presentation, recommendations are offered on how AI awareness can be integrated into educational practice, how transparent and sustainable institutional policies can be developed, and how the responsible and transparent use of AI in higher education can be effectively supported.

Keywords:

artificial intelligence, AI-generated content, text generation, higher education, academic integrity, content detection

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

E-mail:

konferencia@alverad.hu

Web:

https://bgk.uni-obuda.hu/alverad-banki-kiberkonferencia-2025/

https://bgk.uni-obuda.hu/en/alverad-banki-international-conference-on-cybersecurity-and-research-development/

The conference is organized by

Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering

Alverad Technology Focus R&D&I Business Unit

2025.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT