Agenda:
Speech 1
Time: 10:10-11:40

Volodymyr Ilibman
Manager of cybersecurity, Cisco.

EXPERIENCE OF USING CYBERSECURITY SENSORS FOR CRITICAL INFRASTRUCTURE REMOTE MONITORING

Speech 2
Time: 10:40-11:10

Andrii Lytvynov
Network security engineer MUK Group Company, Kyiv, Ukraine. CCNA, CCNA(RS), CNMA.

DRIVING THE REVOLUTION OF SECURE ACCESS EVERYWHERE

Today's workforce expects seamless access to applications wherever they are, on any device. The need for cloud-delivered security service expands daily as users, partners, IoT devices and more each require network access.

Presentation will provide a brief overview of Cisco SASE Architecture as an opportunity to provide secure access to every user to every application from every device.

Speech 3
Time:11:10 – 11:40

Serhii Popov Systems engineer – Cisco.

ENSURING RELIABLE COMMUNICATION USING HYBRID SYSTEMS

There is no only answer to the question which communication system is more reliable - the cloud or the system on the local data centre. The issue becomes even more acute when we talk about communication between different organizations or about additional services such as conference communication. The only solution is systems that have "reflection" both in the cloud and on the local data centre.

Speech 4
Time:11:40 – 12:00

Alexander Kossar Chief designer UADefense Ltd).

SOFTWARE AND HARDWARE COMPLEX FOR PROVIDING SITUATION AWARENESS AND INFORMATION SUPPORT "ICOMWARE"

The software and hardware complex "ICoMWare" is intended for informational support of decision-making by commanders of combat units (units, crews), ensuring their situational awareness and increasing the effectiveness of the interaction of units in a combat environment by creating a single information space on a network-centric basis.

The “ICoMWare”, depending on the version, can be installed both on armored vehicles and automobiles, and operated in any other objects, and its portable version will provide situational awareness to a sabotage-reconnaissance or sniper group, an artillery fire adjuster, an individual soldier, etc. .

The "ICoMWare" PAK is approved for use in the Armed Forces of Ukraine by order of the Ministry of Defense of Ukraine, has a NATO nomenclature number, the code of the item of supply under BK 001-2000 and the level of security guarantees G-2.

The widespread use of the "ICoMWare" will create the basis for the implementation of the concept of conducting combat operations in a single information space in the Armed Forces of Ukraine.

Panel Prospects for the development of telecommunication systems and networks

Agenda:
Speech 1
Time: 12.00-12.15

Andriy Markin, Chief engineer, LLC “Aselsan Ukraine”.

Kostyantyn Ponomarchuk, Senior engineer, LLC “Aselsan Ukraine”.

MODERN TECHNOLOGICAL SOLUTIONS AND DEVELOPMENT TRENDS IN THE FIELD OF MILITARY COMMUNICATIONS OF THE ASELSAN COMPANY

Communication systems of the LTE standard have recently been gaining more and more popularity in the world. In addition, there are already certain samples of military equipment that are manufactured using LTE communication standards. These systems are gaining more and more importance in military affairs. The use of such systems will provide a possibility to increase the capacity of the military command posts in using communication systems, information systems and modern communication services. In addition, the possibility of ensuring the interoperability of such systems with other means of communication, such as software-defined radios (SDR) manufactured by Aselsan and other manufacturers, can be implemented due to the use of a modern internal communication system ICS 6670 manufactured by Aselsan, which can be used as a armored vehicles and in military command posts.

The report provides the results of an analysis of the possibilities of combining communication systems of various standards and the purpose of Aselsan production to increase the capabilities and functionality of military command posts under the conditions of modern warfare.

Speech 2
Time: 12.15 – 12.30

Anatolii Tatarinov, PhD, associated professor, Telecommunication networks and systems department of Military institute of telecommunications and information technologies.

INFOCOMMUNICATION TECHNOLOGIES IN AD HOC NETWORKS FOR C4ISR INFORMATION EXCHANGE BETWEEN MOVING NODES

Abstract

Russia's war against Ukraine demonstrates a significant change in the nature and conditions of conducting hostilities in the tactical zone. The massive use of UAVs significantly reduce a combat control cycle in the C4ISR platform even to seconds or minutes.

It was illustrated that core trend of improving the effectiveness of the strike weapons now is the reliable information exchange in the C4ISR platform between divisions (squads and platoons), operated on armored vehicles during movement. New communication opportunities stimulate interest in mobile adaptive networks.

Taking into account the type and volume of information necessary for the implementation of the C4ISR control cycle, it was justified ad hoc network topology for shortest path of information exchange between armored objects in the units (squads platoon, company) for actual distances between them, and the required line bandwidth. It was shown that ad hoc network should automatically discovering and tracking moving nodes (armored vehicles) should operates with a narrow beam, fast switching, directional antenna for 360 degree plus aerial coverage. Also,automatic in-band neighbor discovery does not require operator intervention to establish links.

The report substantiates the use of adaptive algorithms of channel resources management at the physical, data, and network layers of the OSI model to ensure reliability and security of communication.

Provided information about special military grade broadband radio access equipment in the 2.3-6.0 GHz band, which was proposed for the MoU and the General Staff of Ukraine for testing and solution elaboration.

Speech 3
Time: 12.30-12.45

Ivan Kalashnikov. Head of Training Department Radio Satcom Group LLC, Kyiv, Ukraine.

LERTING NETWORKS USING VHF / UHF RADIOSTATIONS HARRIS RF-7800V AND RF-7850M

Speech about the relevance and necessity of alerting networks and the possibility of their implementation with available means.

Speech 4
Time: 12.45 – 13.00

Serhii Shtanenko, doctoral student of the scientific and organizational department, Military Institute of Telecommunication and Information Technologies named after the Heroes of Kruty Kyiv, Ukraine.

DESIGN OF ADAPTIVE EMBEDDED SYSTEMS IN THE CONTEXT OF INCREASING THE SURVIVABILITY OF THE CONTROL SYSTEM OF COMPLEX OBJECTS AND TECHNOLOGICAL PROCESSES

Abstract

The report proposes a approach to designing secure adaptive embedded systems which is based on their ability to restore their proper functionality by way of reconfiguring hardware components, this process being based on the results of self-control. This approach includes two stages. The first stage involves the initial allocation of tasks to a system's hierarchy levels and nodes followed by their reallocation caused by the system failure in the wake of adverse exposure. The second stage sees the reconfiguration of the system implemented to restore its proper functionality by means of automatic hardware reprogramming.

Panel Cyber security

Agenda:
Speech 1
Time: 13.00-13.30

Vladyslav Chevardin, doctor in technical science, senior researcher. Head of Cyber security department Military institute of telecommunications and information technologies.

MODERN TRENDS DEVELOPMENT IN CYBER SECURITY DOMAIN BASED ON ACTUAL CYBER THREATS

Abstract

An analysis of relationships, cause-and-effect relationships of political decisions, aggravation of interstate relations and the conflicts that followed them showed the great importance and influence of hybrid acts of military-political aggression against Ukraine.

The failure of the planned blitzkriegs, transforming into lengthy and lengthy military operations, is completely dependent on funding, material and information support, and the cyber security of the information and communication systems of the state.

The current state in which the military aggression of the Russian Federation against Ukraine has led has shown the enormous role of information and communication systems, which are used as a platform for the formation of an information surface, obtaining intelligence information, transmitting information for command and control of troops and systems of weapons and military equipment.

The report presents the results of an analysis of the cybersecurity of connections to the Internet of citizens of Ukraine, formed propositions regarding the increase in the cybersecurity of information and communication systems of the state, presented a promising version of an alternative environment for transmitting secure messages for information and communication systems of the state.

Speech 2
Time: 13.30-14.00

Tomas Mogodia, master of science in Middlesex University UKl. NATO Joint Force Command Brunssum Computer Network Defense Branch Head (LTU).

Darlin Jean-Francois, master of science from Missouri university of science and technology (USA). NATO Joint Force Command Brunssum Computer Network Defense Section Head (USA).

DEFENSIVE CYBER OPERATIONS AS A PART OF MILITARY OPERATIONS

Abstract

Presentation will provide a brief overview of CyberSpace as a domain of military operations. Provide insights in importance of Defensive Cyber Operations and its role in supporting overall Commanders mission on the battlefield.

Speech 3
Time: 14.00-14.30

Igor Linkov, Senior Scientific and Technical Manager with the US Army Engineer Research and Development Center (ERDC), and Adjunct Professor with Carnegie Mellon University. US Army Corps of Engineers, Engineer Research and Development Center, 696 Virginia Rd.,Concord, MA 01742, USA.

RESILIENCE IN CYBER AND SOCIAL DOMAINS OF COMPLEX SYSTEMS UNDER ATTACKS

Abstract

Digital interconnectedness has revolutionized how we acquire information and make decisions, fundamentally changing the process by which information spreads through society. While such digital interconnectedness has generated tens of billions of dollars of business revenue each year and has vastly improved social connectivity, it also raises the potential for deliberate misuses of digital systems to wreak havoc upon at-risk or unsuspecting users. The capacity of an organization -- be it a government, company or society in general - - to recover from and adapt to the shifting landscape of threats is known as resilience.

Dr. Igor Linkov will present an overview of resilience and risk within complex, interrelated systems and the development of a framework to manage and measure system resilience. He will present tools to assess the resilience of supply and value chains and present examples to illustrate application of these tools in complex networks. He will discuss the implications of his work for evaluating and managing risk and resilience in information and social domains.

Speech 4
Time: 14.30-15.00

Vyacheslav Kharchenko, doctor in technical science, professor. KhAI, Department of Computer Systems, Networks and Cybersecurity, Kharkiv, Ukraine.

AUTONOMOUS MOBILE SYSTEMS, INTERNET OF SMART THINGS, ARTIFICIAL INTELLIGENCE: SYNERGY FOR CYBERSECURITY AND SAFETY

Abstract

The report overviews problems and solutions of utilizing Artificial Intelligence (AI), Internet of Things, especially Smart Things (IoST), to ensure the safety and cybersecurity of autonomous transport systems (ATSs) in different domains such as aviation, space, and maritime as well as objects of critical infrastructures, first of all, NPP I&Cs and smart grids. The results presented are based on the several on-going projects that are developed by Department of Computer Systems. Networks and Cybersecurity, National Aerospace University KhAI, in particular:

- R&D Project ECHO “European Network of Cybersecurity Centres and Competence Hub for Innovation & Operations”, 2019-2023 (funded by EU Program Horizon 2020);

- R&D&I Project AvioCore 4.0 “German-Ukrainian Core of Excellence in Digitization Research in Domains Industry 4.0 (KhAI, Kharkiv), 2021-2024(funded by German Government);

- R&E Project CyberEDU “MSc and PhD Studies and Research Activities in Cybersecurity of Industrial Control Systems” (funded by Swedish Institute, Stockholm);

- National R&D projects dedicated to development and research:

• Dependable UAV Fleets for Intelligent Monitoring Systems of Critical Objects (2021-2023),

• Methods and technologies for Dependable Industrial IoT (2022-2023),

• Safety and Cybersecurity of SMR Digital Infrastructure (2022-2024) (funded by Ministry of Education and Science of Ukraine) and others.

Speech 5
Time: 15.00-15.30

Lyudmila Kovalchuk, doctor in technical science, professor. National Technical University of Ukraine ”Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

Roman Oliynykov, doctor in technical science, professor V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.

A GRINDING ATTACK ON SLOT LEADERS ELECTION PROCEDURE FOR POS-BASED BLOCKCHAINS WITH ON-CHAIN RANDOMNESS GENERATIONs.

Abstract

In this paper we formulate simple and generalized versions of grinding attack on the procedure of bakers election in Tezos protocol. We obtained formulas for probabilities of both versions of this attack and calculated corresponding numerical results for different stake ratio of adversary. The results obtained show that to get a half or more blocks in a whole cycle, the adversary need to have stake ratio not less than 0.44p to implement a simple version of attack and not less than 0.4p to implement its generalized version.

Speech 6
Time: 15.30-16.00

Ivan Gorbenko, doctor of Technical Sciences, Professor. Chairman of the Board of PJSC “Institute of Information Technologies”, Professor of Security of Information Systems and Technologies Department in V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.

RISK MITIGATION FOR VULNERABLE CRYPTOGRAPHIC SYSTEMS, DEVELOPMENT STATUS, STANDARDIZATION AND IMPLEMENTATION OF SUSTAINABLE POST-QUANTUM CRYPTO PRIMITIVES AT THE INTERNATIONAL AND NATIONAL LEVELS

Abstract

In this paper the object of the study is the processes of reducing the risk of vulnerable (existing) cryptosystems, the development, standardization and implementation of standardized

stable post-quantum cryptoprimitives of asymmetric encryption, electronic signature and key encapsulation protocols at the international and levels.

The subject of research is the methods of synthesis and methods of evaluation, comparative analysis and application of new evidence-proof national and international standardized cryptoprimitives of asymmetric encryption, electronic signature and key encapsulation protocols at the international and national levels.

Speech 7
Time: 16.00-16.30

Sergiy Gnatyuk, doctor of Technical Sciences, Professor. National Aviation University, Kyiv, Ukraine. Scientific Cyber Security Association of Ukraine. https://scsa.org.ua/

QKD-BASED SECURITY FOR 5G NETWORKS AND OTHER SECTORS OF CRITICAL INFORMATION INFRASTRUCTURE OF THE STATE

Abstract

Today, traditional security methods (in particular, cryptographic algorithms) do not fully protect against all currently known attacks, they are potentially vulnerable to attacks based on quantum algorithms. These methods are based on the fundamental impossibility of an attacker to solve some complex mathematical problem (unordered database search, factorization, logarithm in large discrete fields etc.) in polynomial time. But the increase in the computational power of advanced ICT as well as the potential "quantum computer in the hands of an attacker" is a security and privacy threat and it encourages the search for alternative security methods, which will secure the post-quantum period. Such alternative approaches can be methods of quantum and post-quantum cryptography. Quantum Cryptography (Quantum Key Distribution, QKD) does not depend on the computational power of an attacker, uses the specific unique properties of quantum particles and is based on the inviolability of the laws of quantum physics. The main advantages of QKD are the ability to define an attacker and ensure information and theoretical security. QKD includes the following protocols: protocols using single (non-entangled) qubits and qudits (d-level quantum systems, d>2); protocols using phase coding; protocols using entangled states; decoy states protocols and others.

World`s leading QKD company ID Quantique has developed many QKD systems, QRNGs, Quantum-Safe security devices as well as implemented these systems in different sectors of critical infrastructure of the state.

QKD-based post-quantum period security system will be presented and analyzed. Impact of Quantum computing on cryptography (secret key cryptography, public key cryptography, hash functions) will be assessed and analyzed. The methods of QKD integration into different 5G network slices as well as other critical infrastructures will be shown and explained.