Information & Security

ISIJ Monitor
vol. 46, no. 3 (2020): 337-340
https://doi.org/10.11610/isij.4625

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

ISIJ Monitor

DIGILIENCE 2020 Abstracts

The second international scientific conference "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE 2020) will take place in the Naval Academy in Varna, Bulgaria. Here the reader can find the titles and abstracts of the papers that do not appear in the two pre-conference volumes of *Information & Security: An International Journal*.

30 September 2020

Plenary Session I

Salvador Llopis Sanchez, European Defence Agency

Digital Modernisation in Defence: Communications and Information Systems Challenges

A digital transformation of the European Armed Forces requires the setting up of a structured and scalable process to ensure mission readiness. Modern implementations of fielded systems coexist with legacy systems. A plethora of platforms, nodes and information sources integrate a hyper connected battlefield. This article analyses the challenges in seeking harmonized solutions in the field of communications and information systems and especially in the tactical edge which is one of the most demanding areas in terms of real-time information sharing. Tactical communications enable an extension of the mission network perimeter up to individual combatants in a contested and congested environment. In the advent of a cognitive era, emerging technologies such as artificial intelligence combined with cloud computing or the internet of things are at the core of this transformation.

Education and Training for Cyber Resilience

(Parallel Session, Track 1)

Mitko Bogdanoski and Metodi Hadji Janev

Leadership Playbook for the Digital Age: Preparing the Western Balkan Leadership for the Digital Transformation

The ongoing digital transformation caused by emerging technologies poses novel challenges but also opportunities. Western Balkan (WB) leaders are lagging behind the ongoing processes of this transformation. The article argues that WB leaders need to comprehend digital transformation and use this process to improve governance, boost the economy and address existing social challenges.

Radka Nacheva, Adam Stecyk, and Pavel Petrov, *An Accessibility Heuristic Evaluation of Bulgarian and Polish Academic Web Sites: Visually Impaired Users' Perspective*

Accessibility issues are actively involved in the field of information and communication technologies. To improve human-machine interfaces, it is necessary to study the specifics of the interactions of people with special needs, including to improve their security of access to various digital re-sources. Thanks to the state of the art, people with disabilities have wide access to the Internet, including educational resources. The aim of this paper is to propose an approach for the heuristics evaluation of web accessibility based on the analytic hierarchy process (AHP) method. As there are many groups of people with disabilities, to narrow the scope of this study, we turn our attention to the perspective of the visually impaired users. To approve the approach, the authoring team applies it using Bulgarian and Polish academic websites.

Novel Conceptual Approaches and Solutions

(Parallel Session, Track 2)

Konrad Wrona, *Towards Data-centric Security for NATO Operations*

Providing efficient data protection and information sharing capability across different security domains, belonging to NATO, the Nations and specific Communities of Interest (COI), is of paramount importance for effective execution of NATO operations. Current information protection practices rely to large extent on network-layer mechanism for compartmentalisation of information and separation between different COIs. This leads to segregation of networks into separate network domains and the implementation of perimeter defence at the boundaries of these domains. Data-centric security (DCS) architecture rather than focusing on network perimeter defence focuses on securing access to the data itself. DCS represents a new concept for protection of data within IT systems. It introduces a comprehensive set of security measures, involving both passive and reactive measures, which can be configured to address various data protection and information sharing scenarios relevant to NATO in both short and long term. The proposed generic architecture is based on the NATO C3 Taxonomy and the NATO Communication and Information System Security Capability Breakdown.

Cyber Situational Awareness and Information Exchange

(Parallel Session, Track 2)

Daniel Ota and Okan Topçu

Distributed Ledger-Based Trustful Information Exchange on the Tactical Level

Fast, secure, and tamper-proof information sharing between NATO units on a need-to-know basis is crucial. Data quality and integrity are core needs but al-so resilience to failures and manipulations. The core idea of this paper is to use distributed ledger technology to allow a secure information exchange between Command and Control Information Systems of different NATO nations and non-NATO stakeholders such as non-NATO nations or mission observers. Moreover, the distributed ledger supports available NATO standards and formats for data exchange and storage.

1 October 2020

Plenary Session II

Nahim Fazal, CounterCraft, UK

The Power of Cyber Deception

How cyber deception can be used to build up the cyber resilience of organisations in a post lockdown economy, when the availability of online systems is a business imperative? The presentation will discuss the topic of moving the cyber kill chain to the left to enable business resilience and finally how deception shifts the current security paradigm.

Protecting Critical Infrastructures from Cyberattacks

(Parallel Session, Track 1)

Mariia Dorosh and Mariia Voitsekhovska

Functional Modelling of the Organization's ISC State Monitoring System during Project Implementation

Given the situation when recently there is a mass transition to remote work through quarantine, there are new challenges to protect information at another level. Working from home significantly increases existing information security risks and creates new ones that need to be identified and monitored. Thus, the issue of creating information systems for monitoring the level of information security of the organization has recently become increasingly important.

The paper proposes a functional model of the organization's ISC state monitoring system, which determines the input and output parameters, management and implementation of processes. The model may be used in the further development of information systems to solve both individual problems and to create a comprehensive automated monitoring system. Within the framework of the constructed model it is possible to single out project activity, which has such features as: temporality, distribution in time and space, diversity of tasks. In this case, the assessment of information security should take into account the maturity stages of such systems presented in the article. It serves to evaluate the level of development of information security systems of all the project participants and to form an integrated secure information system of the project in the general security system of the organization.

2 October 2020

Big Data and Artificial Intelligence for Cybersecurity

(Parallel Session, Track 2)

Petar Tomov, Iliyan Zankinski and Todor Balabanov

Cybersecurity in Donated Distributed Computing for Evolutionary Algorithms

Donated distributed computing, also known as volunteer computing, is a form of distributed computing that is organized as a public donation of calculating resources. Donated calculating power can involve thousands of separate CPUs and it can achieve the performance of a supercomputer. In most of the cases donated distrib-

uted computing is organized by open source software, which can lead to the involvement of many more volunteers. This research focuses on cybersecurity issues when donated distributed computing is used for optimization with evolutionary algorithms.

Petya Ivanova and Todor Tagarev

Challenges and Opportunities for Network Intrusion Detection in a Big Data Environment

Advanced data storage and processing technologies allow to accumulate logs, network flows and system events from various sources in terabytes of heterogeneous data. This paper presents the state of the art in data pre-processing, feature selection, and the application of a variety of machine learning methods for intrusion detection. It outlines the main challenges in big data analytics and the opportunities provided by combining the outputs of several methods to increase the accuracy of detection and decrease the number of false alarms. The authors propose an architecture of an intrusion detection system combining offline machine learning and dynamic processing of data streams.

Alla Hrebennyk and Elena Trunova

Modelling a Multi-agent Protection System of an Enterprise Network

The paper considers approaches to distribute functions of a corporate network protection system between a set of informational modules – agents, that will ensure mobility, adaptability and fault tolerance of a multi-agent protection system. The analysis of classes of MAS agents by their functionality is conducted. The integration of MAS in corporate networks is based on the distribution of corporate network components between agents which are responsible for their protection. Internal and external information flows caused by user and attacker actions are used to reproduce network activity processes. By involving sets that simulate the behaviour of a regular user, an attacker and a component, the set of MAS agents has been extended to include the following sets: user agent; intruder agent; agent component. The modelling of the MAS agents was conducted with using of the Unified Modelling Language, in particular, the state diagram is constructed and the algorithms of classical agents are described in details: protection agent and counteraction agent, and new ones: user agent, intruder agent, component agent.

It is noted that the proposed approach has a number of advantages, namely: the components of a typical corporate network are distributed across several nodes, so MAS agents will also operate on different nodes, which will ensure the saving and mobility of computing resources; the use of MAS will allow to adapt to changes in the network architecture easily; the creation of new agents provides flexibility of the solution and high scalability; due to the distributed work of agents, the fault tolerance of the system increases: it is harder to attack and disable than systems with a single security server. Management of the entire corporate security system (CSS) can be organized centrally by combining multiple agents using an integration information bus.