AN OVERVIEW OF HASH FUNCTIONS BASED ON NEURAL NETWORKS

Ján ASTALOŠ, Miloš OČKAY, Radoslav FORGÁČ

Abstract: Increasing availability of hardware solutions for calculation of hash functions and the evolution of quantum computers bring the demand for strong cryptographic hash functions, resistant to brute-force attacks. One of the possible approaches is to utilize the properties of neural networks to construct hash functions. The authors of this paper point out the use of neural networks for hashing. On the other hand, they draw the attention to the lack of independent cryptanalysis that would confirm the safety of the neural network approaches.

Keywords: Hash function; Neural network; Chaotic maps; Cryptanalysis; Cryptography; Digital signature.

PREVENTIVE DIAGNOSTICS OF THE COMMON RAIL FUEL SYSTEM INJECTORS

Pavol LUKÁŠIK, Miroslav MARKO

Abstract: Fuel system and electronic systems of the compression-ignition engines belong to the highest failure rates group and to the most economically demanding items in modern vehicles. From this viewpoint they deserve a greater attention in order to prevent break downs, failures and their premature wear. Modern diagnostic tools provide us lots of essential information about current system condition via electronic control units. This issue also relates to company vehicle - Citroën Jumpy 2.0 HDi (Common Rail), which has been used for more than 12 years by Department of Mechanical Engineering (Armed Forces Academy of general Milan Rastislav Štefánik, Liptovský Mikuláš, Demänová). It is recommended to run the diagnostics of the fuel system and its regular monitoring in spite of low mileage (45 500 km). This article deals with actual condition of the fuel system, its issues and recommendations for further operation.

Keywords: Compression-ignition engine; Common Rail; Injector; Nozzle; Diagnostics; Fuel additive.

POSSIBILITIES OF IMPLEMENTATION OF FRIENDLY UNITS´ MANEUVER IN THE COMMON OPERATIONAL PICTURE

Jan NOHEL, Zdeněk FLASAR, Petr STODOLA

Abstract: The article describes the possibilities of the use of information sharing on the network of computer workstations when planning the maneuver routes of a group of cooperating units with the task to attack the same target in a military operation. The key factor for gaining operational superiority over the enemy in this situation is a rapid and accurate processing of all relevant information about the overall battlefield situation. The appropriate solution to this problem is the use of the MCS CZ software, which calculates the optimal maneuver route of the unit based on intelligence information.

Keywords: Information; Situation awareness; Networking; Passability; Maneuver.

USE OF DATA MINING FOR NETWORK BEHAVIOR ANALYSIS OF SELECTED OPERATING SYSTEMS

Július BARÁTH

Abstract: The aim of this paper is to use data mining techniques to obtain characteristic behavior patterns of operating systems with a focus on the communication observed by a remote observer. Network communication of selected operating systems is observed, and the list of contacted targets is recorded. Based on the list, we try to identify the type of operating system used or a group of installed applications. Obtained data can be used for passive reconnaissance of remote networks, detection of possible undesirable leaks of information, filtering of selected communication, etc.

Keywords: Network analysis; Data mining; Operating systems; SIEM; NetFlow.

SMALL UNMANNED AERIAL VEHICLES – THREATS AND DEFENCE AGAINST THEM

Jakub VILÍMEK

Abstract: The article discusses actual small UAVs (Unmanned Aerial Vehicles) threats and ways of defence against them. The introduction contains UAVs regulations in the Czech Republic. The literature review of relevant papers in the UAV threats and defence follows. The third part is about off-the-shelf and professional UAVs, which can be misused to attack. The core of this article describes three vital processes for planning UAV protection: detection, identification and elimination. The goal of the article is to define vital questions, which has to be answered before designing any UAV protection system. The correct answers to these questions depend on the protected area, assets, etc.

Keywords: UAV; UAS; Threat; Detection; Protection; Sensors.

COOPERATION BETWEEN EU AND THE USA IN THEIR POLICY TOWARDS RUSSIA

Marek HARGAŠ

Abstract: The article is focused on the legislative and institutional background of the mutual cooperation of the EU
and the USA within their policy framework towards Russia. It also briefly points out the use of sanctions as one of the main tools.

Keywords: European Union; USA; Russia; Sanctions; Security.