Testing of Utilities for Finding Vulnerabilities in the Machine Code of Telecommunication Devices

Mikhail Buinevich*, Konstantin Izrailov*, Andrei Vladyko*

*The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Russian Federation, Saint-Petersburg, 22-1 Prospekt Bolshevikov

bmv1958@yandex.ru, konstantin.izrailov@mail.ru, vladyko@bk.ru

***Abstract*— The article is devoted to the authors' machine code algorithmization utility to find vulnerabilities in telecommunica-tion devices. The utility is compared with its closest analogue – the IDA Pro software and its plug-in – Hex-Rays. The paper presents the key tests that are used for such comparison and the results of software tools operation for them. The formalized out-come of the comparative analysis justifies the advantages of the authors' utility for solving this task.**

***Keyword*— vulnerability, machine code, algorithmization, IDA Pro, utility testing**

Mikhail Buinevich was born in 1958 in the USSR. He received education of the military engineer of electronic engineering.

He served in the naval fleet and government agencies for information security. He held classes at various universities.
His research interests include methods of information security.
He has more than 100 scientific works. His primary publications are as follows:
1. M.V. Buinevich and others. Safety provision of high-security objects of the naval fleet in relation to damage effects in crisis and emergency situations in peacetime./ Under the editorship of the admiral V.S. Vysotskii.– Saint Petersburg: Publishing house ELMOR, 2008.– 300 p.
2. M.V. Buinevich and others. Provision of organizational and technical support of stability of function and safety of general communications network./ Under the general editorship of S.M. Dotsenko.– Saint Petersburg: Publishing house SPbSUT, 2013.– 142 p.

At the present time Dr. Prof. Buinevich is the professor of Bonch-Bruevich Saint-Petersburg State University of Telecommunications.

Konstantin Izrailov was born in 1979 in the city of Saint Petersburg (Russia). In 1996 he graduated from Saint Petersburg State Polytechnic University, Physical and Mechanical Department.

At the moment he is a researcher of Bonch-Bruevich Saint-Petersburg State University of Telecommunications. He has about 30 published articles; he is an author of 3 scientific and research works and has a patent on the software tool. His scientific interests include information security, search of vulnerabilities in machine code, reverse engineering and telecommunication devices.

Mr. Izrailov has the title of the best postgraduate student of SPbSUT in 2012 and is the presidential scholar in 2013.

Andrei Vladyko (IEEE member (M'14)) acquired his degree of PhD at Komsomolsk-on-Amur State Technical University, Russia in 2001.

At present he is a head of R&D department of The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint-Petersburg, Russia.

His major interests include Control Systems, Internet of Things, Ubiquitous Sensor Network, Information & Network Security, Software-Defined Networking.