Method and Prototype of Utility for Partial Recovering Source Code for Low-Level and Medium-Level Vulnerability Search

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 describes a automated method for searching of low-level and medium-level vulnerabilities in machine code, which is based on its partial recovering. Vulnerability search is positioned in the field of telecommunication devices. All various and typical vulnerabilities in source code and algorithms for its search is given. The article contains examples of usage method and its utility. There is forecast to develop methods and utilities in the near future.**

Keyword— **machine code, reverse-engineering, static analyzer, telecommunication devices, vulnerability**

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.

Dr. Prof. Buinevich, at the present time, is the professor of the Protected Communications System Chair of Saint Petersburg State University of Telecommunications (SPbSUT).

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 postgraduate student of the Protected Communications System Chair of Saint Petersburg State University of Telecommunications (SPbSUT). He has about 20 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 the Candidate of Sciences at Komsomolsk-on-Amur State Technical University, Russia in 2001.
At present he is a head of the Scientific Work Organization and Researchers Training Administration of Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint-Petersburg, Russia. His major interests include control systems, soft computing, communication networks, network security management.