Method and Utility for Recovering Code Algorithms of Telecommunication Devices for Vulnerability Search

Mikhail Buinevich*, Konstantin Izrailov**

*The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Russian Federation, Russia Federation, Saint-Petersburg, 192242, 23-4 Bucharestskaya, apt.41

**The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Russian Federation, Russia Federation, Saint-Petersburg, 192212, 17-2 Budapeshtskaya, apt.9

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

***Abstract*— The article describes a method for searching vulnerabilities in machine code based on the analysis of its algorithmized representation obtained with the help of an utility being a part of the method. Vulnerability search falls within the field of telecommunication devices. Phase-by-phase description of the method is discussed, as well as the software architecture of the utility and their limitations in terms of application and preliminary effectiveness estimate results. A forecast is given as to developing the method and the utility in the near future.**

***Keyword*—binary codes, information security, reverse engineering and decompilation, program language extension, telecommunications**

Mikhail Buinevich was born in 1958 in the USSR. He studied to be a military engineer of electronics.

He served in the Navy and government agencies, ensuring data protection; he taught at various universities. His research interests lie in the field of the methodology of information security. He has over 100 publications. Major publications are as follows:

1. Buinevich M.V. and other, “Ensuring the safety of critical facilities of the Navy from the effects of damaging factors in crisis and emergency situations in peacetime”// Under Ed. Admiral V.S. Vysotsky. – St. Petersburg: Publishing House of ELMOR, 2008.– 300 pp.
2. Buinevich M.V. and other, “Organizational and technical sustainability of the operation and safety of the public telecommunications network“// Under Society Ed. S.M. Dotsenko. – St. Petersburg: Publishing House of the SPbSUT, 2013.– 142 pp.

Prof. Buinevich, DSc in Engineering (Russian Scientific Degree “Doctor of Technical Sciences”) is currently a Professor of Department of Information Security of Telecommunication Systems at the St. Petersburg State University of Telecommunications (SPbSUT).

Konstantin Izrailov was born in 1979 in St. Petersburg (Russia). In 1996, he graduated from the of Physics and Mechanics Department of the St. Petersburg State Polytechnic University (SPbSTU).

Currently, he is a postgraduate student at the Chair of the Department of Information Security of Telecommunications System of St. Petersburg State University of Telecommunications (SPbSUT). He has published about 10 articles, participated in the execution of 2 scientific researches and holds a patent on a software tool. His research interests are the information security, reverse-engineering (decompilation) and telecommunication devices.

Mr. Izrailov was ranked the best postgraduate student of the year 2012 of SPbSUT and was a Presidential Scholar in 2013.