Company

LLC “Laboratory of Network Technologies” (LLC LNT) is a small innovative enterprise, founded in 2004. LLC LNT was started on the base of the joint research laboratory of Moscow Engineering Physics Institute and the commercial company “KONTUR Soft” when the R&D project “Computer Network Audit System (CNAS)” was selected in a competition to take part in a support program for innovations arranged by the Foundation for Assistance to Small Innovative Enterprises.

Nowadays the company consists of 14 specialists, with 40% involved in R&D activities. Employees of LLC LNT are engineer-mathematicians, certified programmers and technicians with strong professional qualification and wide working experience. Senior, diploma and PhD students participate in R&D projects under supervision of the qualified company’s staff.

Over the last five years among others the following main results were achieved: 3 R&D projects were successfully completed and registered in Russian Scientific Technical Information Center; 3 certificates on official registration of computer programs were obtained in Federal Institute for Industrial Property of the Federal Service for Intellectual Property, Patents and Trademarks; a test-bed for controlled and real-life experiments was built; research results were implemented in the prototype software system “Security Locator” and put into trial operation.

Area of business

LLC LNT is mainly focused on research and development activities in the field of information security and operability control of distributed heterogeneous IT- infrastructures, aimed to increase efficiency of network behavior analysis and novel security threat detection. Completed R&D activities provided the following results: a required experimental base; the unique methodology for network device abnormal states detection based on multidimensional statistical analysis of structured traffic information; the software system “Security Locator”, which provides continuous monitoring, behavior analysis and anomaly detection in IP-networks, as well as operation data and analysis results visualization capabilities.

Also LLC LNT uses own software and methodological developments in another business area. In addition to R&D activities the company provides IT-consulting and outsourcing services, including network security assurance (risks analysis, security policy preparation, security systems deployment), configuration and maintenance of computer networks, dedicated servers and services, network operability control and performance optimization (http://www.ntlab.ru).

Software solutions

The software system “Security Locator” enables detection of network states that are different from a normal operation state. Such deviations from the “normal” can be a signal of potential security violations, including unauthorized access and abuse of network resources, network performance degradation and hardware failures, caused by unintentional errors or by malicious activity of an intruder. “Security Locator” allows a security administrator to immediately identify and take appropriate actions against internal and external threats. This software system provides a real picture of what really happens in the network and helps network administrators to optimize its infrastructure in order to meet increasing users’ demands of network services and performance.

The developed software can be used by various user groups in many application domains: by administrators to diagnose network “health” and control if network resources are properly protected; by researchers to approbate new methods in testing and real-life environments; by teachers of network technologies for students’ practical training within education programs. Wide area of application and high quality of the solution are provided by a professional level of the team and implementation of the latest development technologies and tools.

Research methods and development technologies

In order to achieve required analysis efficiency and detection accuracy it is necessary to consider specificity of information security violation identification problem. Therefore development of network anomaly detection and classification techniques is based on application of complex mathematical methods to real network traffic data and security events obtained during extensive controlled and real-life experiments. Different methods of data pre-processing, multidimensional statistical analysis and soft computing are used in this research. Also applicability of immune models and algorithms, adopting basic concepts of the human immune system, is under investigation. Interest in artificial immune systems is justified by unique properties of the human immune system related to its ability to protect an organism against continuous attacks of infectious agents, including previously unknown. The most interesting immune concepts are distributed and decentralized, self-organizing defense mechanisms, adaptation to changing conditions and learning new antigens, high fault-tolerance – all compliant with recent requirements to network intrusion detection systems.

The software system “Security Locator” which implements the research results was developed using RUP (Rational Unified Processes) methodology. The development cycle includes requirements analysis, design, implementation and comprehensive testing of software components in testing and real-life environments. Program implementation of the developed

anomaly detection techniques involves the following technologies:

- Platform: Java2 J2EE; Apache Tomcat.
- Object-oriented representation: Hibernate, Java Persistence API (JPA).
- Web layer: Java Server Faces (JSF), JSP & Servlets.
- Graphics and reports: jFreeChart, JasperReports, iReport.
- Data storage: Oracle, Postgre, MySQL.
- Traffic capture: C++, libpcap (Windows, Linux, FreeBSD).
- Other: XML-RPC, Log4J, Java3D VecMath, JaMa.