Analytical Modeling of Mobile Banking Attacks based on a stochastic network conversion technique

Igor Saenko[1], Oleg Lauta[2], and Igor Kotenko[1,3*]
[1]St. Petersburg Institute for Informatics and Automation (SPIIRAS)
39, 14 Liniya, St. Petersburg, Russia
ibsaen, ivkote@comsec.spb.ru
[2]St. Petersburg Signal academy
3, Tichoretsky prospekt, Saint-Petersburg, Russia
o.lauta@yandex.ru
[3]St. Petersburg National Research University of Information Technologies, Mechanics and Optics
49, Kronverkskiy prospekt, Saint-Petersburg, Russia

Abstract

Now the quantity and complexity of mobile banking attacks strongly increase. It brings extensive economic damage and requires increase of mobile security level. Development of reliable analytical models that adequately represent real attack implementation processes in different conditions is necessary for effective protection against mobile banking attacks. The paper considers an approach to analytical modeling of mobile banking attacks based on a stochastic network conversion technique. The essence of this technique consists in changeover of a set of elementary branches of a stochastic network by one equivalent branch and the subsequent determination of an equivalent function of the network, and the initial moments and distribution functions of the computer attack implementation time. Advantages of the offered method are the high speed of modeling, high reliability, and high sensitivity of results to initial data change. The experimental assessment of the proposed method has confirmed its sufficiently high efficiency.

Keywords: Mobile Security, Attack Modeling, Mobile Banking Attack, Stochastic Networks, Laplace Transform

1 Introduction

Nowadays, more and more people use smart phones and pads for web browsing, communication in social networks, shopping and banking operations in the Internet. At the same time, malefactors even more often attack mobile devices, using at the same time new threats against smart phones and mobile devices.

The last research works show that personal smart phones of staff of the companies represent the greatest threat for corporate data security and are a headache for experts in the sphere of IT-security [17]. According to the results of investigations of the SophosLabs company, more than 650,000 separate samples of malicious software for Android [19] are known now. The most widespread harmful objects found in the Android smart phones are the following three main groups: (1) SMS Trojans; (2) advertising modules; (3) exploits for receiving access of the root level to smart phones. Malicious applications are found in app stores, such as Google Play, Amazon and others. In 2014, daily 2000 new Android malware samples were found. Thus, the malicious software of smart phones and pads grew quickly for a short period. It tends to a further strong growth.

IT CoNvergence PRActice (INPRA), volume: 4, number: 4 (December 2016), pp. 1-10
*Corresponding author: Laboratory of Computer Security Problems, St. Petersburg, Institute for Informatics and Automation (SPIIRAS), 39, 14 Liniya, St. Petersburg, Russia

Many commercial banks and payment service providers offer different methods of protection of user financial operations. User authenticity checking with use of USB tokens and one-time passwords, confirmation of operations by means of codes sent to phone, etc. are related to them. Nevertheless, malefactors develop new programs that allow bypassing these protective measures [12]. A characteristic example of such program is the malicious application ZITMO (Zeus-In-The-MObile). It is intended for attack against mobile phones, works in a tandem with the malicious application ZeuS [6] and can bypass the system of two-factor authentication used by commercial banks [4].

The assessment of implementation risk of mobile banking attacks requires creation of analytical models which allow to analyze efficiently the dependences of probabilistic parameters. Many approaches for creation of probabilistic models of attacks are known. However, a technique based on conversion of stochastic networks obtains an increasing popularity now [10]. This technique differs in higher accuracy and stability of generated solutions. Besides, it is simpler to prepare the initial data for this approach. Therefore, the purpose of the paper is creation and analysis of a new analytical model for mobile banking attacks based on this technique. As an example, the attack of ZITMO type is selected.

Thus, the theoretical contribution of the paper consists in development of a new approach to creation of analytical models of computer attacks based on conversion of stochastic networks, and its application for mobile attacks.

The further structure of the paper is as follows. In Section 2 the review of related work is given. Section 3 discusses the mathematical foundations of the approach suggested. The order of creation of a stochastic network is given. The stochastic network conversion technique is described. Section 4 demonstrates the results of experiments. Conclusions about the presented results and the directions of future research are presented in Section 5.

2 Related Work

Stochastic analytical modeling and simulation of computer attacks is more and more used now in computer security systems to substantiate the choice of preferred security (counter-measure) solution. Stochastic discrete event simulation systems, such as COMNET [2] and OPNET [8], operate on this basis. Functioning of these systems is founded on event based simulation of queuing networks. These networks can be considered as one of types of stochastic networks. As modeling and simulation of queuing systems of arbitrary type requires considerable computing expenses, this aspect is the essential shortcoming restricting the application of stochastic discrete event simulation in security systems.

In [11] a tool CAMIAC (Cyber Attack Modeling and Impact Assessment Component) is offered for attack simulation and analysis. This tool realizes methods of attack impact evaluation based on the analysis of attack graphs and stochastic modeling and simulation of different attacks and countermeasures. However, stochastic models in this tool do not allow to calculate attack time distribution functions.

In [7] a stochastic attack simulator is offered. This simulator is based on use of calculation of situations and implementation of goal-directed procedure invocations. These innovations allow the simulator to execute very flexible representation of attack actions and simulate intelligent attackers. However, a lack of this approach is the need to specify attack scenarios on special situation calculus language.

In [1] a stochastic security framework is offered. It considers vulnerabilities and calculates security metrics values. Computation is based on non-homogeneous Markov models and Markov reward models. This work considers the temporal aspect connected with vulnerabilities and a vulnerability lifecycle model. However, we think the application of these models for analytical simulation of attacks will involve considerable computing costs.

[5] offers the approach to formation of stochastic attack models that allows to consider attack distri-

bution on parallel branches. In this work, particular mobile security scenarios are considered. However, the computation carried out in this work is based only on application of the main theorems of the probability theory. Therefore, they cannot be considered as sufficient to determine attack implementation time distribution functions.

In [13] different examples of stochastic and statistical models for different tasks in the field of computer science are reviewed. As the main mathematical abstraction, the discrete Markov chains are used. We consider these chains as a variety of stochastic networks. However, the scenarios connected to attack modeling are not considered in this work. Sufficiently interesting results in the field of security are received by use of generative stochastic networks. In [21] the approach to classification based on this type of stochastic networks is provided, and in [3] the technique for training of such networks based on the algorithm of the reverse distribution is offered. These works show that stochastic networks are rather powerful modeling and simulation tool. However, the issues connected to attack modeling and simulation are not considered in these works.

Thus, the analysis of related work shows that stochastic analytical modeling and simulation is of great importance for generation of counter-measures in modern security systems. Stochastic models should provide possibilities to generate time distribution functions for implementation of attacks and their separate stages with minimum computing expenses. Besides, they should provide high flexibility and to be applicable for modeling and simulation of any type attack. The approaches considered above not fully meet these requirements. The stochastic network conversion technique described below allows to eliminate this shortcoming.

3 Mathematical Background

3.1 A Stochastic Network for the ZITMO Attack

The stochastic network is understood as a set of interconnected nodes and branches (edges) which connection corresponds to algorithm of functioning of the investigated system. At the same time, the network is realized, if some subset of branches, which implementation time is selected according to probabilistic distribution [18], is executed. The stochastic network is not a model of a system. It is a model of the process that is realized by this system. A complex process is decomposed on elementary processes, each of which is characterized by a distribution function, an average time and its dispersion.

The logic and sequence of processes execution is determined by a bipolar network. The network comprises input, intermediate and output nodes connected by edges. A set of elementary processes corresponds to edges, and conditions of their execution – to nodes.

Each node executes two functions. One function is an input one. It defines a condition (i.e. logical expression) for execution. Function "excluding OR", "OR" and "AND" are considered usually as input functions. The second function is an output one. It defines which operation after this node will be executed. Output function can be of deterministic or probabilistic type. In case of deterministic output, all branches, beginning from this node, are realized with probability, equal to 1. In case of probabilistic output at best one output branch is used. The input node of the network executes only preceding output function, and an output node only input one.

Transmission function is defined for each edge. This function plays a role of a conditional characteristic function. It represents Laplace transform for a probability density function for a time of an elementary process fulfillment [20].

The stochastic network contains a set of loops. The loop is a connected closed sequence of stochastic network oriented branches, where each node is common exactly for two branches or for the branch connecting node to itself.

As an example of a stochastic network creation we will select an attack like ZITMO. As for the first time the attack of this type was found and distributed in Euro Zone countries, according to the terminology of some analytical companies it was named as Eurograbber [9]. Implementation of this attack has the following stages [14]:

- The malefactor directs to a mobile device of the victim a SMS-message with the request to complete the "banking software security upgrade". Suppose that duration of this stage has the distribution function $W(t)$ and the average time $\overline{t_W}$.
- The victim with the probability P_n follows the link in the message. The mobile device is infected by the malicious application ZITMO for the average time $\overline{t_L}$ with the time distribution function $L(t)$.
- The trojan ZITMO redirects the login and the password of the victim to the malefactor to transfer the money from his account for the average time $\overline{t_M}$ with the time distribution function $M(t)$.
- For authorization the bank sends SMS-message, containing "transaction authorization number", to the mobile device of the victim. The phone, infected with ZITMO, sends this message to the malefactor for the average time $\overline{t_D}$ with the time distribution function $D(t)$. This action allows the malefactor to confirm the transaction and to take control on the money of the victim.
- If the victim did not follow the link in the message, then with the probability $(1–P_n)$ the malefactor repeatedly directs the message for the average time $\overline{t_Z}$ with the time distribution function $Z(t)$.

The stochastic network, reflecting the stages of ZITMO, listed above, is represented in Figure 1. All nodes of the network have the input functions "Excluding OR". The functions $w(s)$, $l(s)$, $m(s)$, $d(s)$, and $z(s)$, which are on the output of the stochastic network nodes, are the *equivalent functions* which are defined by application of Laplace transform to the time distribution functions $W(t)$, $L(t)$, $M(t)$, $D(t)$, and $Z(t)$, respectively.

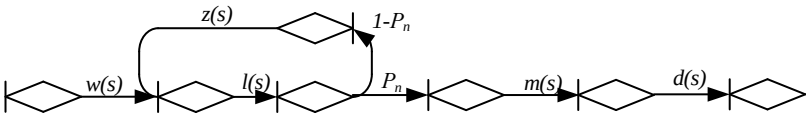


Figure 1: Stochastic network of the malicious application ZITMO

3.2 A Technique of Stochastic Network Conversion for the ZITMO Attack

The *equivalent function*, saving in its structure the distribution parameters and the interaction logic of elementary stochastic processes is the result of conversion of the stochastic network. The equivalent function allows to define the first moments of stochastic runtime of the target process. If the distribution function of the attack stage time is designated as $G(t)$, then the equivalent function $g(s)$ is calculated as follows:

$$g(s) = \int_0^\infty exp(-st)d[G(t)]. \quad (1)$$

If we apply the inverse Laplace transformation to the equivalent function of some process, then the result of such transformation is the probability density function for this process runtime.

The *essence of this technique* consists in changeover of a set of elementary branches of a stochastic network by one equivalent branch and the subsequent determination of the equivalent function of the

network, and the initial moments and the distribution function of the analyzed process implementation time, i.e. computer attack time.

The equivalent function of the k-th order loop is defined as follows

$$Q_k(s) = \prod_{i=1}^{k} Q_i(s). \tag{2}$$

where $Qi_i(s)$ – the equivalent function of the$i$-th order loop defined as the multiplication of equivalent functions of the branches included in this loop.

Let us connect conditionally the output and input of the network. Then for the required equivalent function $h(s)$ the expression $h(s) = 1/Q_a(s)$ is fair, where $Q_a(s)$ is the equivalent function of the input of the network.

When connecting the output and input of the network, it becomes closed. In this case, for determination of the equivalent function of the initial network it is possible to use the Mason's equation for closed graphs [16]:

$$H = 1 + \sum_{k=1}^{K} (-1)^k Q_k(s) = 0. \tag{3}$$

where K – the maximum order of the loops included in the stochastic network. Now we will define all loops in the stochastic network given in Figure 1.

According to (2) the first loop has the equivalent function $w(s) \cdot m(s) \cdot l(s) \cdot P_n \cdot d(s)/h(s)$. The second loop has the equivalent function $(1 - P_n) \cdot z(s) \cdot l(s)$.

There are no loops of the second and higher orders.

Then the equation (3) can be written as follows:

$$1 - w(s) \cdot m(s) \cdot l(s) \cdot P_n \cdot d(s)/h(s) - (1 - P_n) \cdot z(s) \cdot l(s) = 0. \tag{4}$$

The equivalent function of all network in this case is as follows:

$$h(s) = \frac{w(s) \cdot m(s) \cdot l(s) \cdot P_n \cdot d(s)}{1 - (1 - P_n) \cdot z(s) \cdot l(s)}. \tag{5}$$

Using Laplace transform and Heaviside expansion theorem [15], the probability distribution function of implementation time for the computer attack ZITMO can be defined as follows:

$$F(t) = \sum_{k=1}^{5} \frac{w \cdot l \cdot P_n \cdot m \cdot d \cdot (z + s_k)}{\varphi(s_k)} \cdot \frac{1 - exp[s_k t]}{-(s_k)}. \tag{6}$$

where $\varphi(s_k)$ – the reference designation of a polynom in the denominator; s_k – the expansion pole of k-th order; $w = (\overline{t_W})^{-1}$; $l = (\overline{t_L})^{-1}$; $m = (\overline{t_M})^{-1}$; $d = (\overline{t_D})^{-1}$; $z = (\overline{t_Z})^{-1}$. The polynom $\varphi(s_k)$ has following look:

$$\varphi(s_k) = (w + s_k) \cdot (d + s_k) \cdot (m + s_k) \cdot [(l + s_k) \cdot (z + s_k) - (1 - P_n) \cdot z \cdot l]. \tag{7}$$

The average time $\overline{T}$ spent for implementation of the malicious application ZITMO is defined as follows:

$$\overline{T} = \sum_{k=1}^{5} \frac{w \cdot l \cdot P_n \cdot m \cdot d \cdot (z + s_k)}{\varphi'(s_k)}) \cdot \frac{1 - exp[s_k t]}{s_k^2}. \tag{8}$$

where $\varphi'(s_k)$ – the value of the derivative of the polynom in the denominator in the point s_k.

The values of equivalent functions calculated for the stochastic network depicted in Figure 1 and the time distribution functions for each stage of the attack ZITMO are represented in Table 1.

Table 1: Functions to assess the duration of the ZITMO attack stages

Stage #	Stage content	Equivalent function	Time distribution function
1	Sending the message by the malefactor	$w(s) = \frac{w}{w+s}$	$W(t) = 1 - exp[-wt]$
2	Transition on the link and infection of the mobile device	$l(s) = \frac{l}{l+s}$	$L(t) = 1 - exp[-lt]$
3	Redirection of the login and the password to the malefactor	$m(s) = \frac{m}{m+s}$	$M(t) = 1 - exp[-mt]$
4	Redirection of the transaction authorization number to the malefactor	$d(s) = \frac{d}{d+s}$	$D(t) = 1 - exp[-dt]$
5	Repeated direction of the message by the malefactor	$z(s) = \frac{z}{z+s}$	$Z(t) = 1 - exp[-zt]$

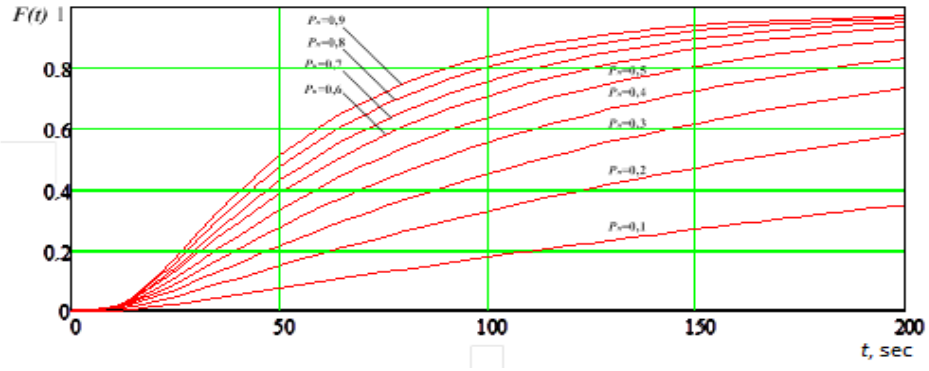
4 Experimental results and discussion

Results of calculations of $F(t)$ and $\overline{T}$ are represented in the form of dependences in Figure 2. The following values of the average times of the ZITMO attack stage implementation (justified experimentally) are used as initial data: $\bar{t}_W = 5$ sec, $\bar{t}_L = 10$ sec, $\bar{t}_M = 5$ sec, $\bar{t}_D = 40$ sec, and $\bar{t}_Z = 4$ sec. At the same time, the probability of the user transition changes in a broad range: $P_n = 0.1 \ldots 0.9$. The analysis of the received results allows to draw the following conclusions:

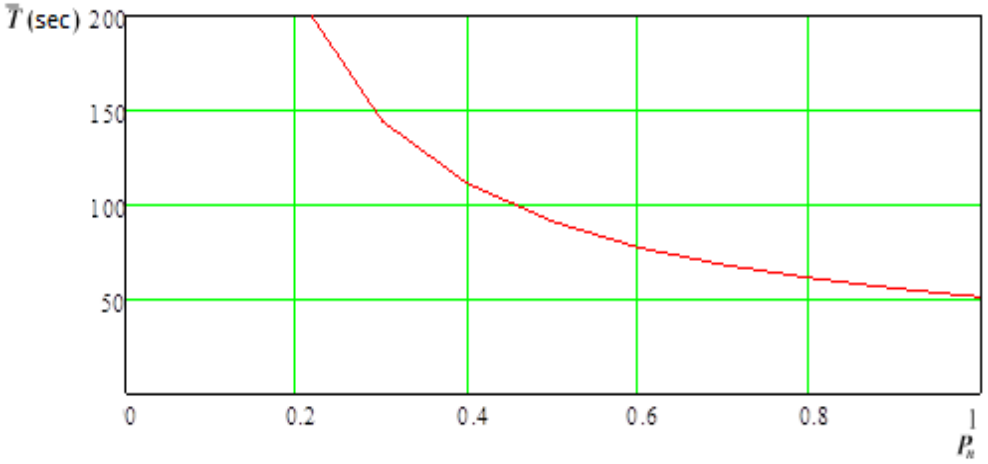
- the average time of computer attack implementation for the ZITMO malicious application, if the probability of the user transition to the link $P_n = 0.8$, makes 60 seconds;
- in case of reduction of the probability of the user transition to the link P_n, the average time of the computer attack implementation increases according to the exponential law;
- if the user follows the link in the message with probability $P_n = 0.5$, then the time of computer attack implementation with probability 0.8 will not exceed 2.5 minutes, and if $P_n = 0.7$, then it will not exceed 2 minutes.

Thus, the received dependences allow to estimate the influence of the time and the probability of the victim transition to the link on the efficiency of the ZITMO malicious application implementation. The reduction of the probability P_n of the victim transition to the link in the message considerably increases the average time of the malicious application implementation.

The resulted model has following features. First, for receiving a resultant distribution function for the attack implementation time it is enough to know only the first moments (mean values) of times defining



a) Dependence of the integral probability distribution on the time of malicious application implementation



b) Dependence of the average time of malicious application implementation on the probability of the transition according to the link

Figure 2: Probabilistic and time response characteristics of the malicious application ZITMO

duration of particular attack stages. Second, the average times of the first, third and fourth stages of the attack play an identical role in analytical model that is visible from (6–8).

To check these features, a series of experiments on the developed simulation tool was carried out. The tool is based on the MATLAB R2013a. The following modules were a part of the simulation tool: (1) initial data input, (2) generator of durations of attack stages, (3) the manager. The module of initial data input determined the values $\bar{t}_W$, $\bar{t}_L$, $\bar{t}_M$, $\bar{t}_D$, and $\bar{t}_Z$ and P_n. The generator created randomly the implementation times for attack stages by the pseudorandom number generator. The manager created a random value for the attack implementation time. For these purposes, the manager used the values received on outputs of the generator and the probability P_n.

The received experimental results are given in Table 2. For each value of the probability P_n, 100 experiments were made. At the same time, the values of average times of particular attack stages, considered for the dependences provided in Figure 2, were used. As it can be seen from Table 2, the error of an assessment of the attack implementation time does not exceed 5 percent. Therefore, the offered analytical model and the technique of its formation are sufficiently correct and adequate.

Table 2: Experimental results for average attack implementation times

P_n	**Average model time, sec**	**Simulated time**	
		Average time, sec	Error, %
0,2	250	261	4,4
0,3	140	139	0,7
0,4	118	123	4,2
0,5	97	101	4,1
0,6	76	75	1,3
0,7	68	67	1,5
0,8	60	62	3,3
0,9	55	54	1,8

5 Conclusion

The paper offers a new approach to analytical modeling and simulation of computer attacks based on the stochastic network conversion technique. The essence of this technique consists in changeover of the set of elementary branches of the stochastic network by one equivalent branch and the subsequent determination of the equivalent function of the network, as well as the initial moments and distribution functions of the computer attack implementation time. The evaluation of the offered approach was made for modeling of the ZITMO attack, which is one of the most dangerous among mobile banking attacks. The experimental assessment of the proposed method showed its sufficiently high efficiency.

The advantages of the offered approach are: (1) using as initial data only the initial moments of implementation times for particular attack stages; (2) high speed of modeling; (3) high reliability of modeling results; (4) high sensitivity of results to change of initial data. It is possible to refer the need of training of security administrators to create stochastic networks to a lack of the offered approach. However, this shortcoming quickly disappears and is compensated by the accuracy of modeling of real attack implementation processes. Receiving in an explicit form of analytical expressions allows to use the results of attack modeling to detect the reasons of low security of mobile network elements and to substantiate counteraction measures. The directions of future research are connected with using the offered approach for modeling of complex and target computer attacks against mobile networks and increasing the level of validity of the taken counteraction measures.

Acknowledgments

The work is performed by the grant of RSF #15-11-30029 in St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS).

References

[1] S. Abraham and S. Nair. A predictive framework for cyber security analytics using attack graphs. *International Journal of Computer Networks & Communications*, 7(1):1–17, January 2015.

[2] S. Ahuja. Comnet iii: a network simulation laboratory environment for acourse in communications networks. In *Proc. of the 28th Annual Frontiers in Education Conference (FIE'98), Tempe, Arizona, USA*, pages 1085–1088. IEEE, December 1998.

[3] Y. Bengio, E. Thibodeau-Laufer, and J. Yosinski. Deep generative stochastic networks trainable by backprop. In *Proc. of the 31st International Conference on Machine Learning (ICML'14), Beijing, China*, pages 1–16, June 2014.

[4] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi. Security analysis of mobile two-factor authentication schemes. *Intel Technology Journal*, 18(4):138–161, July 2014.

[5] D. Dudorov, D. Stupples, and M. Newby. Probability analysis of cyber attack paths against business and commercial enterprise systems. In *Proc. of the 2013 European Intelligence and Security Informatics Conference (EISIC'13), Uppsala, Sweden*, pages 38–44. IEEE, August 2013.

[6] N. Etaher, G. R. S. Weir, and M. Alazab. From zeus to zitmo: Trends in banking malware. In *Proc. of the 13th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA'15), Helsinki, Finland*, pages 1386–1391. IEEE, August 2015.

[7] R. P. Goldman. A stochastic model for intrusions. In *Proc. of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID'02), Zurich, Switzerland, LNCS*, volume 2516, pages 199–218. Springer-Verlag, October 2002.

[8] J. Guo, W. Xiang, and S. Wang. Reinforce networking theory with opnet simulation. *Journal of Information Technology Education*, 6:215–226, 2007.

[9] E. Kalige and D. Burkey. A case study of eurograbber: How 36 million euros was stolen via malware. whitepaper, December 2012.

[10] F. Kelly and E. Yudovina. *Stochastic Networks*. Cambridge University Press, 2014.

[11] I. Kotenko and A. Chechulin. A cyber attack modeling and impact assessment framework. In *Proc. of the 5th International Conference on Cyber Conflict (CYCON'13), Tallinn, Estonia*, pages 1–24. IEEE, June 2013.

[12] A. Luvanda, S. Kimani, and M. Kimwaele. Identifying threats associated with man-in-the middle attacks during communications between a mobile device and the back end server in mobile banking applications. *IOSR Journal of Computer Engineering*, 16(2):35–42, March-April 2014.

[13] N. Matloff. *From Algorithms to Z-Scores: Probabilistic and Statistical Modeling in Computer Science*. Orange Grove Books, 2009.

[14] C. Mulliner, R. Borgaonkar, P. Stewin, and J.-P. Seifert. Sms-based one-time passwords: Attacks and defense. In *Proc. of the 10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA'13), Berlin, Germany, LNCS*, volume 7967, pages 150–159. Springer-Verlag, July 2013.

[15] S. S. Petrova. Heaviside and the development of the symbolic calculus. *Archive for History of Exact Sciences*, 37(1):1–23, March 1987.

[16] D. T. Phillips and A. Garcia-Diaz. *Fundamentals of Network Analysis*. Prentice-Hall, 1981.

[17] P. Ruggiero and J. Foote. Cyber threats to mobile phones. Technical report, United States Computer Emergency Readiness Team (US-CERT), 2011.

[18] R. Serfozo. *Introduction to Stochastic Networks (Stochastic Modelling and Applied Probability)*. Springer, 1999.

[19] V. Svajcer. Sophos Mobile Security Threat Report. `https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf`, 2014.

[20] J. L. Williams. *Laplace Transforms (Problem Solvers)*. Allen & Unwin, 1973.

[21] M. Zohrer and F. Pernkopf. General stochastic networks for classification. In *Proc. of the 2014 Neural Information Processing Systems (NIPS'14), Montreal, Canada*, pages 2015–2023, December 2014.

Author Biography

Igor Saenko graduated with honors from St. Petersburg Signal Academy. He obtained the Ph.D. degree in 1992 and the National degree of Doctor of Engineering Science in 2001. He is Professor of computer science and Leading Researcher of the Laboratory of Computer Security Problems of St. Petersburg Institute for Informatics and Automation. He is the author of more than 200 refereed publications and participated in several Russian and international research projects. His main research interests are security policy management, access control, management of virtual computer networks, database management, knowledge modeling, soft and evolutionary computation, information and telecommunication systems.

Oleg Lauta graduated from St. Petersburg Signal Academy. He obtained the Ph.D. degree in 2005. He is Teacher of St. Petersburg Signal Academy. He is the author of more than 50 refereed publications and participated in several Russian research projects. His main research interests are protection of computer networks and counteraction to computer attacks.

Igor Kotenko graduated with honors from St.Petersburg Academy of Space Engineering and St. Petersburg Signal Academy. He obtained the Ph.D. degree in 1990 and the National degree of Doctor of Engineering Science in 1999. He is Professor of computer science and Head of the Laboratory of Computer Security Problems of St. Petersburg Institute for Informatics and Automation. He is the author of more than 200 refereed publications. Igor Kotenko has a high experience in the research on computer network security and participated in several projects on developing new security technologies. For example, he was a project leader in the research projects from the US Air Force research department, via its EOARD (European Office of Aerospace Research and Development) branch, EU FP7 and FP6 Projects, HP, Intel, F-Secure, etc. The research results of Igor Kotenko were tested and implemented in more than fifty Russian research and development projects. The research performed under these contracts was concerned with innovative methods for network intrusion detection, simulation of network attacks, vulnerability assessment, security protocols design, verification and validation of security policy, etc. He has chaired several International conferences and workshops, and serves as editor on multiple editorial boards.