

GERT-NETWORK OF SOURCE CODE VERIFICATION PROCESS FOR CRYPTOGRAPHIC AND OTHER WAYS TO PROTECT DATA

Zhang Liqiang

Department of IT information Centre Neijiang Normal University, Neijiang, China
Chernykh O.

National Technical University «KhPI», Kharkiv, Ukraine

Our study has shown that the process of cryptographic conversion or obfuscation of the source code of software can be represented as a combination of algebraic operations of weighted addition and multiplication.

These algebraic ratios can be formalized as equivalent transformations and *GERT*-network transitions. In practice, in the SW encryption or obfuscation processes, the selection of successive operations is done using a random number sensor. The *GERT*-model of these processes makes it possible to analyze the probabilistic behavior of the software hiding (transformation) system and could be used to estimate the number of options that need to be sorted out when testing software security for cryptographic transformation [1]. We shall consider methods to find these characteristics using an example of the software encryption scheme shown in Fig. 1.

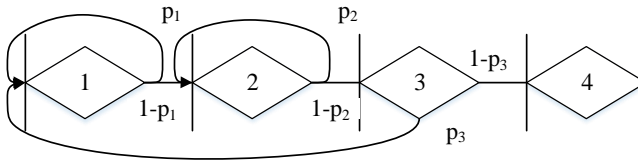


Fig. 1. Software encryption scheme for a generalized *GERT*-network

Let us find an average of the number of conversions that are being performed. As a basis, we shall take the exponential law of distribution of the random value of the time of the transformation and, accordingly, the moment-generating functions of branches are equal to e^s . Then the equivalent *W*-function of the *GERT*-encryption network of software is equal to

$$W_{k_E}(s) = \frac{q_1 q_2 q_3 e^{4s}}{1 - (p_1 + p_2) e^s + p_1 p_2 e^{2s} - q_1 q_2 p_3 e^{3s}}, \quad (1)$$

where $q_1=1-p_1$, $q_2=1-p_2$, $q_3=1-p_3$ are the probabilities of branch selection (1, 2), (2, 3), (3, 4) in the scheme shown in Fig. 2.5, respectively.

Expression (1) can determine the average number of N conversions performed and its variance D_N .

$$N = \frac{3\gamma_1 + 2\gamma_2 - \gamma_3 + 1}{\gamma_1}, \quad D_N = \frac{(2\gamma_2 - \gamma_3 + 1)^2 - \gamma_1(1 - 4\gamma_2 + \gamma_3)}{\gamma_1^2}. \quad (2)$$

Using the Mathcad specialized mathematical package, we shall calculate some combinations of q_1-q_3 probabilities and the corresponding N and D_N values. It has been proven in [2] that the time of encryption and decryption depends on the time

each functional conversion is performed. In addition, the cited work gives an example of modeling the cryptographic system R_1 , the basis of the formalization of which is the Chinese theorem about the remnants. In this case, the following expression was obtained to analyze the time of the R_1 system:

$$Wk_E^{(R_1)}(s) = e^{(\beta s + 0.5k_1 D s^2)}, \quad \beta = k_1 + [(k_1 + 1)t_{\text{до}} + (k_2^2 + 1)t_{\text{ум}} + (k_3 - 1)t_{\text{сн}}]; \quad (3)$$

k_i is the number of integer division, multiplication, and addition operations, respectively, normalized for τ ($\tau=10$ for example); t_{div} is the time it takes for integer division operations; t_{mul} is the time it takes for multiplication operations; t_{sum} is the time it takes for addition operations.

We shall use (3) to find the equivalent W -function of the source code verification process for cryptographic and other ways to protect the data. For the cases set in Table 2 (case 1— $q_1=0.1$, $q_2=0.4$, $q_3=0.4$, case 2— $q_1=0.3$, $q_2=0.1$, $q_3=0.5$. For both cases, $D_N=9$, $k_1=k_2=k_3=2$), we shall obtain the W -function of R_1 conversion time:

$$Wk_E^{(R_1)}(s) = e^{(1.376s + 16.9s^2)}. \quad (4)$$

Then the equivalent W -function of the time of the process of testing a cryptographically converted software product

$$Wk_E(s) = \frac{q_1 q_2 q_3 e^{5.04s + 67.6s^2}}{1 - (p_1 + p_2)e^{1.38s + 16.9s^2} + p_1 p_2 e^{2.76s + 33.8s^2} - q_1 q_2 p_3 e^{4.14s + 50.7s^2}}, \quad (5)$$

References

1. Семенов С.Г., Сур О.О Математична модель системи криптографічного захисту електронних повідомлень на основі GERT-мережі Системи управління, навігації та зв'язку»: К.:ЦНДІ навігації і управління, 2012. Вип. 1(21), том 1. С.131-137.
2. Garg Vishal (2014) "Approaches, tools and techniques for security testing" <https://www.3pillarglobal.com/insights/approaches-tools-techniques-for-security-testing>

TESTING PROCESS MATHEMATICAL MODEL FOR PENETRATION INTO COMPUTER SYSTEMS

Cao Weiling

Department of IT information Centre Neijiang Normal University, Neijiang, China
Chernykh O.

National Technical University «KhPI», Kharkiv, Ukraine

Penetration testing services have become increasingly popular in the IT-industry. A number of popular articles [1] set out in some detail the possible approaches and steps that accompany these services. However, these works vast majority consider this cybersecurity assessment type from a view practical point, based on the expertise in various computer and information infrastructures experience. This, in turn, leads to spectrum and increased run time either unreasonable expansion, without ensuring the appropriate assessment quality, or