AGENȚI ADAPTIVI PENTRU IDENTIFICAREA INTUZIUNILOR ÎN SISTEMELE INFORMAȚIONALE

Andrei ȘESTACOV[1*]

[1]Universitatea Tehnică a Moldovei, Facultatea Calculatoare, Informatică și Microelectronică, Departamentul Informatică și Ingineria Sistemelor, SD SCEE, Chișinău, Republica Moldova)

*Autorul corespondent: Andrei Șestacov, andrei.sestacov@army.md

Rezumat. *Atacurile cibernetice DDoS reprezintă o amenințare din ce în ce tot mai mare pentru sistemele informaționale. Sistemele pentru detectarea intruziunilor deja au devenit o componentă obligatorie pentru a asigura securitatea informațională a sistemelor și rețelelor de calcul. În lucrarea de față se pune accentul pe importanța și avantajele aplicării sistemelor imune artificiale pentru identificarea intruziunilor în sistemele informaționale. Aceste sisteme sun considerate Agenți inteligenți care dispun de adaptibilitate, scalabilitate, flexibilitate și exactitate. Evoluția cunoștințelor ale agenților are loc de fiecare dată când este identificat un atac informațional detectat de sistemul imunitar artificial.*

Cuvinte cheie*: atacuri cibernetice, sisteme imune artificiale, sistem de detecție a intruziunilor.*

Modelul sistemului imunitar artificial de identificare a intruziunilor

Funcționalitatea sistemului imunitar artificial (SIA) pentru identificarea indruziunilor în sistemele informaționale este inspirat din comportamentul sistemului imunitar uman (SIU) care prezintă o rețea complexă de celule, procese și organe care lucrează în colaborare pentru a apăra corpul uman de infecții și viruși externi [1,2]. SIU poate identifica milioane de corpuri străine și generează anti-corpuri pentru a le neutraliza.

Utilizarea SIA pentru detectarea intruziunilor este dictată de doi factori decisivi: SIU oferă într-un mod robust, auto-organizat și distribuit corpului uman un nivel sporit de protecție împotriva invadării de către Agenți patogeni; și, la moment nu există o altă alternativă care să ofere soluții mai avantajoase în comparație cu SIA.

Modelul SIA dezvoltat este definit în baza modelului matematic (1):

$$SIA = \{A_I, A_C, A_N, A_K, A_G\}, \quad (1)$$

unde: A_I - Agenți pentru identificarea intruziunilor; A_C - Agenți pentru crearea și menținerii în carantină a apelurilor suspecte; A_N - Agenți pentru neutralizarea apelurilor identificate ca atac cibernetic; A_K - Agenți pentru menținerea și completarea bazei de cunoștințe; A_G - Agenți de gardă, supervizează modul de activitate și de reproducere (clonare, mutație și multiplicare) a agenților A_I, A_C, A_N, A_K.

Mulţumiri. Cercetările fac parte din tematica tezei de doctorat și au fost efectuate cu suportul tehnologic și metodologic oferit de DIIS.

Referinţe

1. UDDIN, M., ALSAQOUR, R., ABDELHAQ, M. Intrusion Detection System to Detect DDoS Attack in Gnutella Hybrid P2P Network. *Indian Journal of Science and Technology. Vol. 6. Issue 2,* 2013. pp. 4045-4057. ISSN:0974-6846.
2. KIM, J.P., BENTLEY, J., AICKELEN, U., GREENSMITH, J., TEDESCO, G., TWYCROSS, J. Immune System Approaches to Intrusion Detection – A Review. *Natural Computing, Springer.* 59p. doi: 10.1007/s11047-006-9026-4.