Metody ilościowe w ocenie bezpieczeństwa informacyjnego

Ryszard Antkiewicz

Wydział Cybernetyki, Wojskowa Akademia Techniczna

Plan wystąpienia

- Pojęcia podstawowe
- Prognozowanie możliwości wystąpienia ataku
- Prognozowanie występowania podatności
- Modele ataku
  - drzewa zdarzeń;
  - model stochastyczny ataku;
- Ochrona danych przed utratą – metody archiwizacji danych, ocena niezawodnościowa
- Ocena skutków ataku – model DoS
- Inne metody monitorowania wykrywania zagrożeń

Bezpieczeństwo informacji

- **Bezpieczeństwo informacji** - stopień uzasadnionego zaufania, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego):
  - ujawnienia,
  - modyfikacji,
  - zniszczenia,
  - uniemożliwienia przetwarzania

  informacji przechowywanej, przetwarzanej i przesyłanej w określonym systemie obiegu informacji (systemie informacyjnym). [Lid]

- **Bezpieczeństwo teleinformatyczne** – stopień uzasadnionego zaufania, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego):
  - ujawnienia,
  - modyfikacji,
  - zniszczenia,
  - uniemożliwienia przetwarzania

  informacji przechowywanej, przetwarzanej i przesyłanej za pomocą systemów teleinformatycznych. [Lid]

Zagrożenia i podatności

- Na bezpieczeństwo zasobów systemu teleinformatycznego mają wpływ zagrożenia i podatności.

- **Zagrożenie** – potencjalne działanie człowieka albo sił wyższych (pożar, powódź, trzęsienie ziemi, awaria techniczna), dotyczące bezpośrednio zasobu systemu teleinformatycznego lub organizacji procesu przetwarzania informacji i mogące spowodować, w zależności od konkretnego atrybutu bezpieczeństwa: tajności, integralności lub dostępności straty proporcjonalne do wagi procesu krytycznego, wspieranego przez zagrożony proces i wykorzystywane w nim zasoby [Lid].

- **Podatność** – wada lub luka w systemie teleinformatycznym, która może być wykorzystana przez zagrożenie do spowodowania szkód w systemie teleinformatycznym lub działalności organizacji PN-I-02000:1998].

Ryzyko – pojęcia podstawowe

- ✓ Następstwem wystąpienia incydentu bezpieczeństwa są wszelkie negatywne skutki dla organizacji i jej systemów teleinformatycznych [Biał]
- ✓ Ryzyko oznacza miarę stopnia zagrożenia bezpieczeństwa informacji. Wyraża się je najczęściej jako iloczyn prawdopodobieństwa wystąpienia incydentu bezpieczeństwa i miary skutków (strat) wynikających z tego incydentu. [Lid]
- ✓ Zabezpieczenia systemu teleinformatycznego to praktyka, procedura lub mechanizm redukujący ryzyko do pewnego akceptowanego poziomu, zwanego ryzykiem szczątkowym [Biał]
- ✓ Sposób postępowania z ryzykiem systemów teleinformatycznych jest treścią procesu zarządzania ryzykiem.

Podstawowe elementy zarządzania ryzykiem

- ✓ Analiza ryzyka
  - ✓ Identyfikacja ryzyka
    - ✓ Zakres analizy ryzyka
    - ✓ Identyfikacja zagrożeń
    - ✓ Podatności
    - ✓ Potencjalne straty
  - ✓ Oszacowanie ryzyka
- ✓ Opracowanie zasad postępowania z ryzykiem w zakresie jego
  - ✓ Unikania
  - ✓ Kontrolowania
  - ✓ Transferu
  - ✓ Retencji
- ✓ Akceptacja ryzyka szczątkowego
- ✓ Monitorowanie ryzyka

Prognozowanie możliwości wystąpienia ataku

Wykorzystanie regresji logistycznej do prognozowania wystąpienia ataku określonego typu wobec systemu stosującego określone zabezpieczenia techniczne i organizacyjne [Das]

- Rozpatrywane typy ataków: **DoS** – denial of Service, **Virus**, **UA** – unauthorized access to the information; **SP** – system penetration; **TPI** – theft of propriety information; **FF** – financial fraud;
- Rozpatrywane typy zabezpieczeń:
  - Techniczne: **IDS** – intrusion detection system, **FW** – firewall; **AVS** – antivirus software; **B-** biometrics;
  - Organizacyjne: **RLE** – reporting to law enforcement; **RLC** - reporting to Legal Council;
  - Finansowe: **ITS** – procent budżetu IT alokowanego na kwestie bezpieczeństwa; **ITO** – procent zadań związanych z bezpieczeństwem informacji outsorsowany;
- Dane z ankiet FBI-CSI realizowanych w latach 1997 - 2010

Prognozowanie możliwości wystąpienia ataku

- ✓ Wykorzystano model regresji logistycznej:

$$P(Y_j = 1 \mid X = x) = \frac{exp(\beta_{0j} + \sum_{i=1}^{n} \beta_{ij} \cdot x_i)}{1 + exp(\beta_{0j} + \sum_{i=1}^{n} \beta_{ij} \cdot x_i)} = \frac{exp(\beta^T x^*)}{1 + exp(\beta^T x^*)}$$

$$\beta = (\beta_0, \beta_1, .., \beta_n)^T, \quad x^* = (1, x_1, .., x_n)^T$$

Table 6a. Coefficients of the Logit Function

	UA	TPI	SP	FF	Virus	DoS
AVS	-	-	-	-	-	-
FW	(-.031) (***)	-	-	-	-	-
IDS	-	-.007 (**)	.006 (*)	-.014 (***)	-	-.021 (***)
B	-.04 (***)	-.062 (***)	-.088 (***)	-	-.111 (**)	-.067 (**)
RLE	-	(.04) (***)	.083 (***)	.031 (***)	.043 (**)	.015 (**)
RLC	.024 (***)	-	-	-	-	-
Dev	10.47	2.13	2.31	2.66	10.08	2.65
Chi Sq	10.26	2.10	2.32	2.8	10.33	2.67

*** p < 0.01 , ** p < 0.05 , * p < 0.1; - = Not Significant

Table 6b. Coefficients of the Logit Function for ITS on Type of attack

	UA	TPI	SP	FF	Virus	DoS
ITS	-.009 (**)	-	-	-.016 (***)	-.028 (***)	-.016 (***)
Deviance	3.066			4.937	18.7	9.2
Chi Sq	3.04			5.5	18.64	9.139

*** p < 0.01 , ** p < 0.05 , - = Not Significant,

Table 6c. Coefficients of the Logit Function for ITO on Type of attack

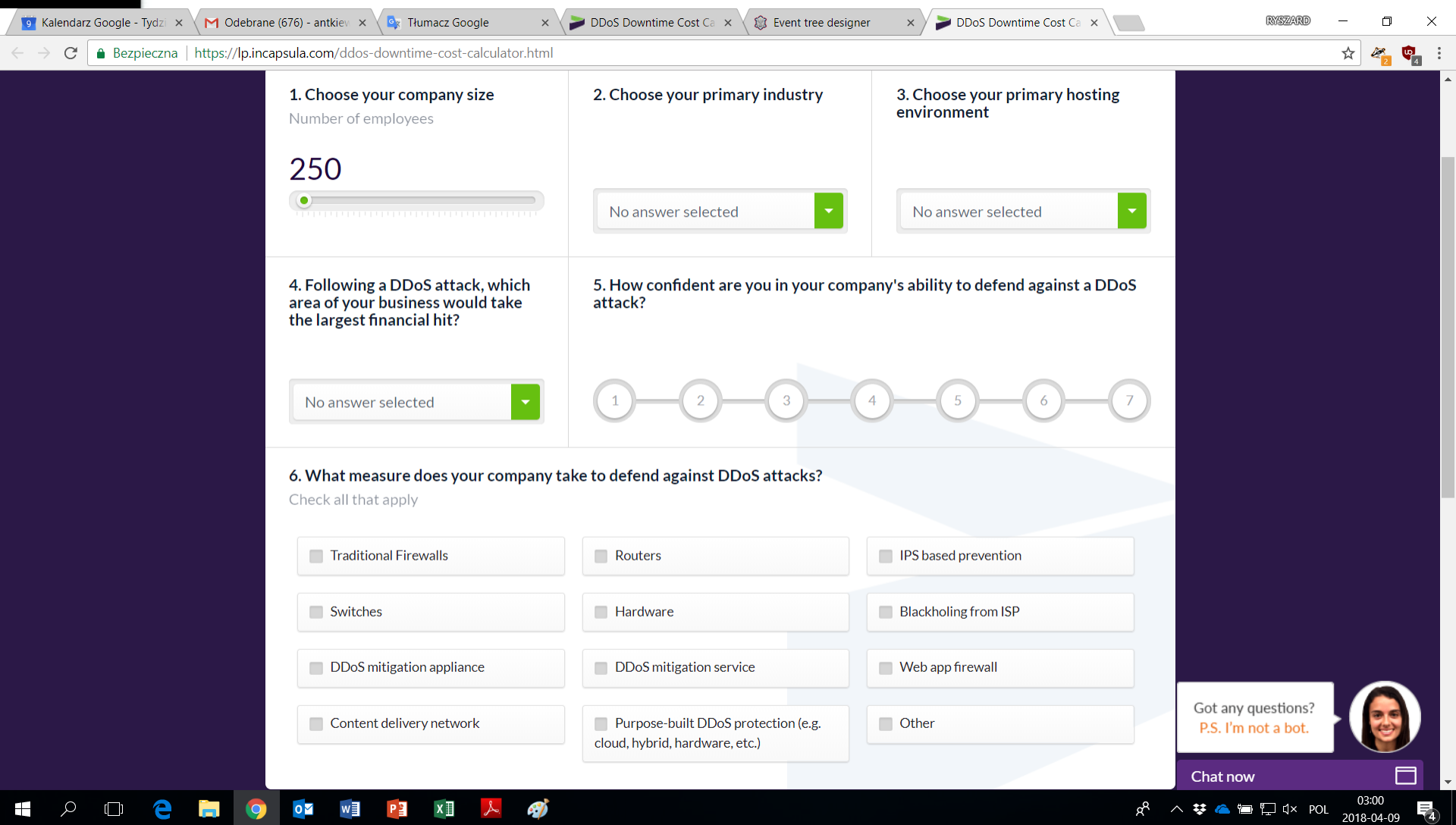
	UA	TPI	SP	FF	Virus	DoS
ITO	-.04 (***)	-.05 (*)	-	-.05 (**)	-.119 (***)	-.056 (***)
Deviance	2.351	.454		5.179	12.57	8.82
Chi Sq	2.39	.467		5.26	12.66	8.89

*** p < 0.01 , ** p < 0.05 , * p < 0.1; - = Not Significant

Prognozowanie możliwości wystąpienia ataku

- ✓ DDoS Downtime Cost Calculator (firma: Imperva)

https://lp.incapsula.com/ddos-downtime-cost-calculator.html



Prognozowanie możliwości wystąpienia ataku

✓ DDoS Downtime Cost Calculator

Register to calculate the downtime cost of DDoS attacks to your organization.

Full Name | Email address | Your Company | Select Country...

RESET | CALCULATE COST

Estimates to be Calculated

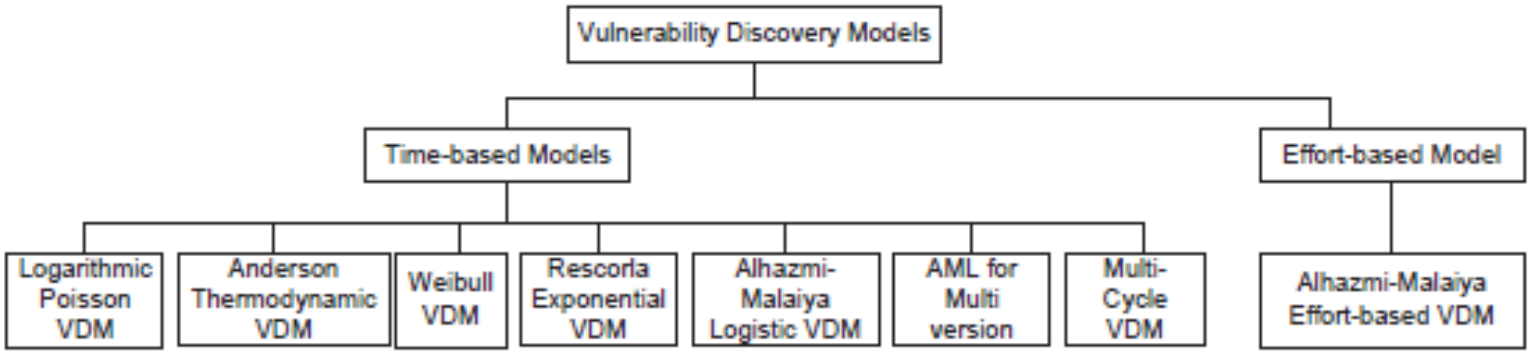
%	%	$	$
Probability of Ever Being Targeted by a DDoS Attack	Probability of Being Targeted by a DDoS Attack Within the Next Year	Expected Annual Cost of DDoS Attack w/o DDoS Attack Protection	Estimated Cost of DDoS Attack Per Hour

IMPERVA INCAPSULA

© 2018 Imperva. All rights reserved. Terms of Use | Privacy Policy

Wykrywanie podatności

- Podatności można potraktować jako podzbiór błędów oprogramowania, powodujących występowania błędów wykonania.
- Opracowane do tej pory modele podatności, bazujące na modelach niezawodności oprogramowania) można sklasyfikować następująco [Younis]



- Model dotyczą mogą dotyczyć dwóch procesów:
  - Proces wykrywania podatności – źródłem danych są przede wszystkim bazy danych podatności; (vulnerability discovery models VDMs)
  - Proces wykorzystania wykrytych podatności – brak wiarygodnych danych, zaatakowane firmy nie upubliczniają wielu ataków (vulnerability exploitation models VEMs) Podatności wykrywane s przez ekspertów. Wykorzystać je mogą również osoby bez wiedzy specjalistycznej.

Alhazmi-Malaiya Logistic Model (AML) [Alhazmi05]

- Przyjmuje się, że intensywność wykrywania podatności spełnia następujące równanie różniczkowe:

$$\frac{d\Omega(t)}{dt} = \mathrm{A}\Omega(t)(\mathrm{B} - \Omega(t))$$

gdzie:

- $\Omega(t)$ - liczba podatności wykrytych w przedziale $(0, t)$
- A, B – stałe modelu, wyznaczane na podstawie danych empirycznych (pomiarowych).

Wyznaczając rozwiązani powyższego równania otrzymujemy zależność:

$$\Omega(t) = \frac{B}{BCe^{-ABt} + 1}$$

gdzie:

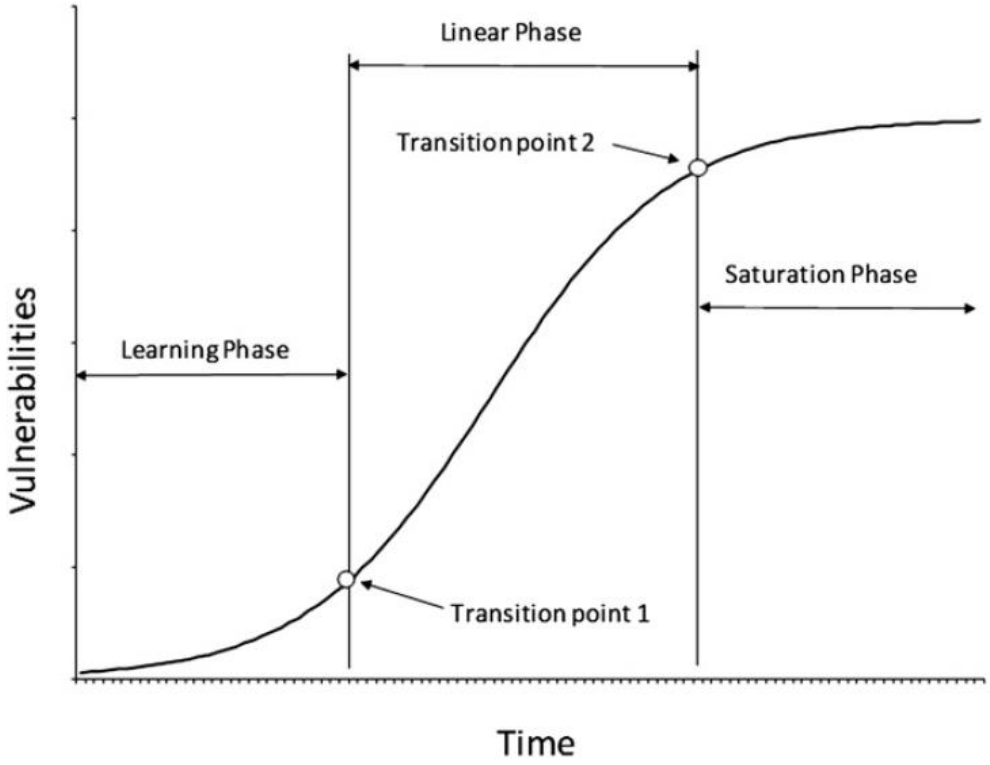
- C – stała całkowania, wynikając z rozwiązania równania różniczkowego, wartość wyznaczana na podstawie danych empirycznych.

Alhazmi-Malaiya Logistic Model (AML) [Alhazmi05]

✓ Uwzględniając zależność:

$$\lim_{t\to+\infty} \Omega(t) = \lim_{t\to+\infty} \frac{B}{BCe^{-ABt}+1} = B$$

Można interpretować wartość parametru B jako całkowitą liczbę podatności w badanym systemie.



$$T_1 = \frac{-\ln\left[\frac{2-\sqrt{3}}{B\cdot C}\right]}{A\cdot B}$$

$$T_2 = \frac{-\ln\left[\frac{2+\sqrt{3}}{B\cdot C}\right]}{A\cdot B}$$

Alhazmi-Malaiya Logistic Model (AML) [Alhazmi06]

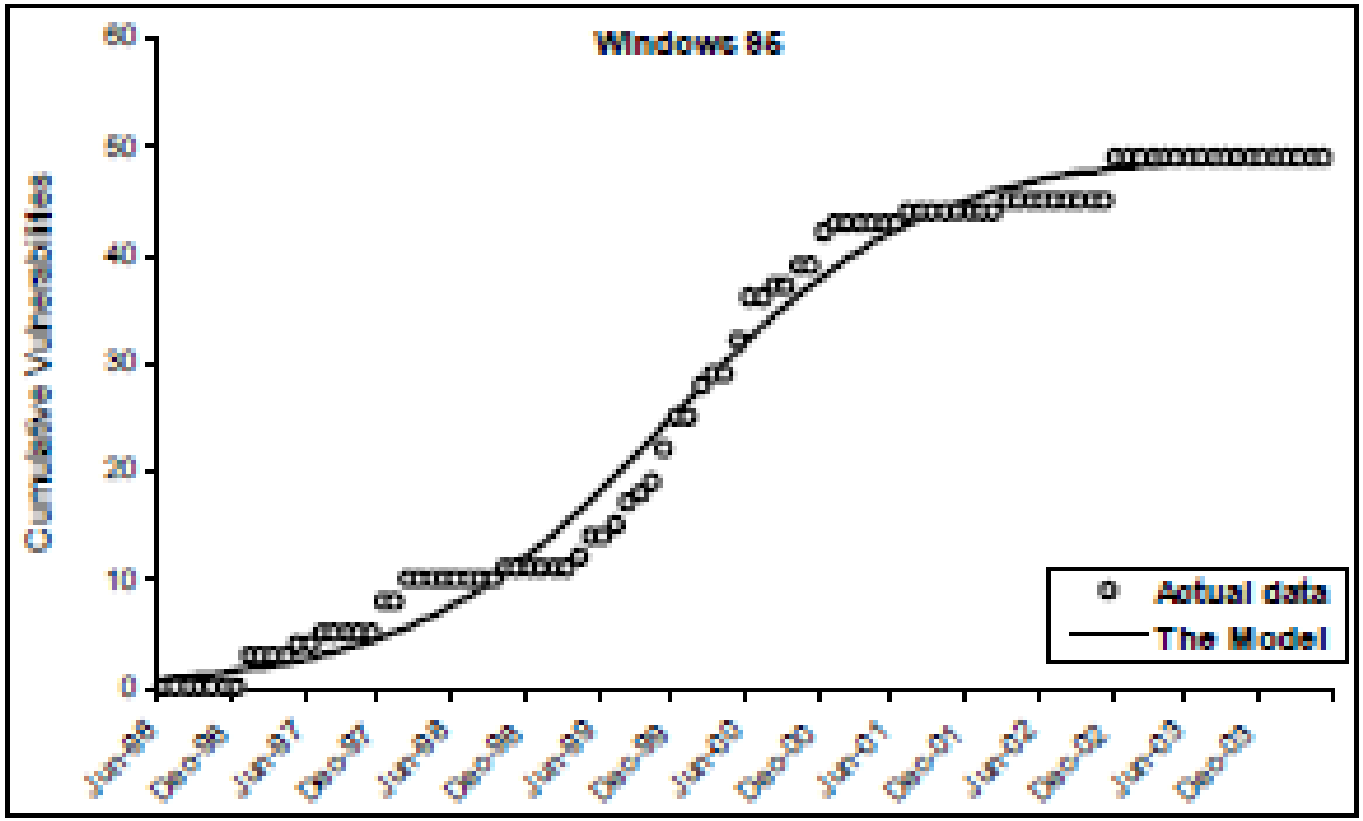


Figure 1 – Alhazmi-Malaiya Logistic (AML) model fitted to Windows 95 vulnerability data set

Stochastyczny model ataku

Rozpatrywany system [Azg]:

System teleinformatyczny składający się z Microsoft SQL Server Database, Microsoft FrontPage Web Server, stacji roboczych. System jest wyposażony w firewall oraz IDS.

- ✓ Typy ataków
  - ✓ Buffer overflow
  - ✓ Man-in-the-middle
  - ✓ SQL injection
  - ✓ Traffic sniffing

Stochastyczny model ataku

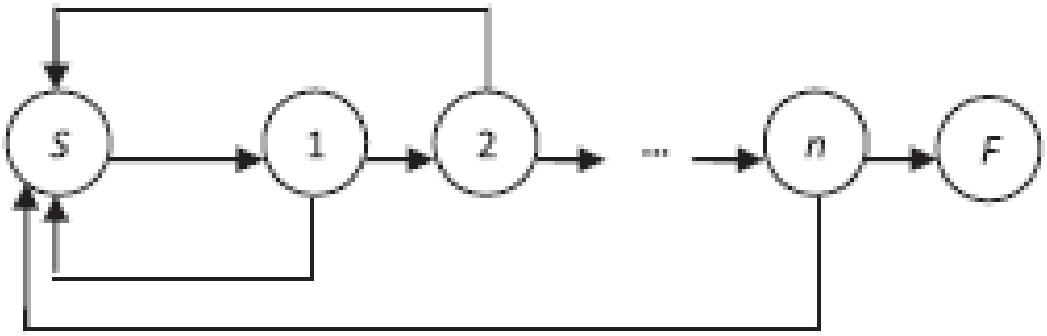
Przykład [Azg]:

- ✓ Wyróżnione fazy ataku typu „Traffic sniffing”:
  - ✓ Identyfikacja podatnej stacji roboczej
  - ✓ Zdalna instalacja złośliwego oprogramowania na wytypowanej stacji roboczej, umożliwiającej przejęcie kontroli nad maszyną
  - ✓ Instalacja sniffera;
  - ✓ Zdalne podsłuchiwanie aktywnych sesji, przechwytywanie i wydobywanie użytecznych informacji – docelowy stan naruszenia bezpieczeństwa

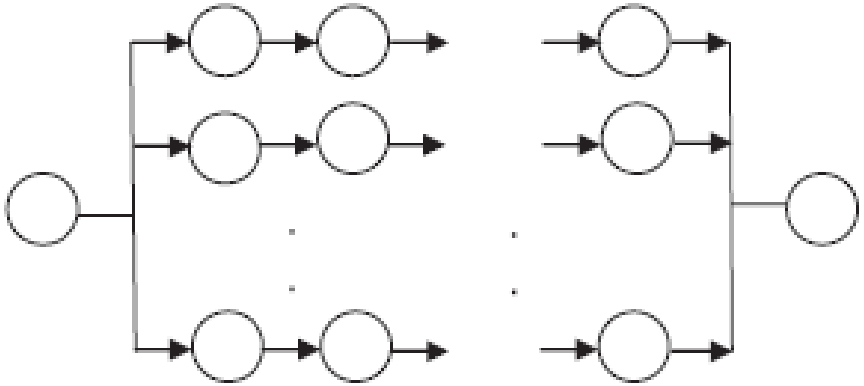
- ✓ Celem modelowania jest wyznaczenie następujących wskaźników:
  - ✓ Rozkład i oczekiwany czas do wystąpienia docelowego stanu naruszenia bezpieczeństwa
  - ✓ Graniczne (stacjonarne) prawdopodobieństwo wystąpienia docelowego stanu naruszenia bezpieczeństwa

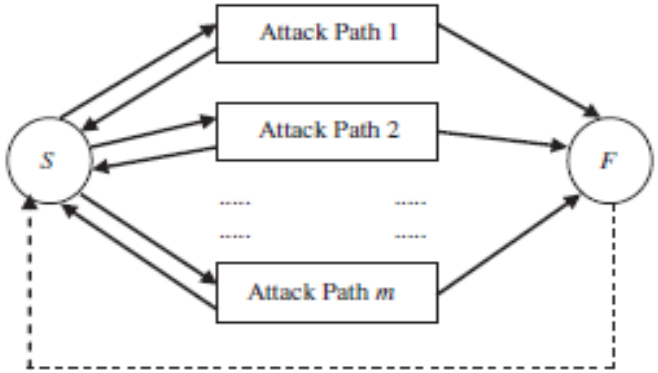
Stochastyczny model ataku

Ilustracja przebiegu pojedynczego ataku jest następujący graf [Azg]:



Powyższy schemat pokazuje pojedynczą ścieżkę ataku. Jeśli w jednym modelu uwzględni się wiele ścieżek ataku (odpowiadających różnym typom ataku) na pojedynczy system, to można to zilustrować to następującymi schematami:





Stochastyczny model ataku

Uwzględniając przyjęte założenia, można zdefiniować proces stochastyczny $Z(t)$, , jako model ataku, którego zbiór stanów określony jest następująco:

$$\boldsymbol{Z} = \{\mathrm{S}, z_{ij}, \mathrm{i} = 1, .., \mathrm{m}, \mathrm{j} = 1, .., n_i, \mathrm{F}\},$$

gdzie:

S – oznacza stan bezpieczny systemu;

F – oznacza stan pełnego złamania zabezpieczeń i uzyskanie przez atakującego pożądanego wyniki ataku;

z_{ij} - stan systemu po wykonaniu *(j-1)* fazy ataku typu *i-tego* i w trakcie realizacji fazy *j-tej.*

Stochastyczny model ataku

$$G_{ij}(\mathrm{t}) = \mathrm{P}\{T_{ij} < \mathrm{t}\} = \mathrm{P}\{\min\{X_{ij}, Y_{ij}\} < \mathrm{t}\} = 1 - \mathrm{P}\{\min\{X_{ij}, Y_{ij}\} \geq \mathrm{t}\} =$$
$$1 - \mathrm{P}\{X_{ij} \geq \mathrm{t}, Y_{ij} \geq \mathrm{t}\} = 1 - \mathrm{P}\{X_{ij} \geq \mathrm{t}\} \cdot P\{Y_{ij} \geq \mathrm{t}\} =$$
$$= 1 - (1 - F_{X_{ij}}(\mathrm{t})) \cdot (1 - F_{Y_{ij}}(\mathrm{t}));$$

$$Q_{z,y}(\mathrm{t}) = \mathrm{P}\{\mathrm{Z}(t_{r+1}) = \mathrm{y}, \theta_{r+1} < \mathrm{t} |\ \mathrm{Z}(t_r) = \mathrm{z},\} \text{ dla } z, y \in \boldsymbol{Z}$$

$$Q_{z,y}(\mathrm{t}) = \begin{cases} P\{X_{ij} > Y_{ij}, Y_{ij} < t\} = \int_0^t (1 - F_{X_{ij}}(\mathrm{u}))\, d\, F_{Y_{ij}}(\mathrm{u}) & z = z_{ij}, y = S \\ P\{X_{ij} < Y_{ij}, X_{ij} < t\} = \int_0^t (1 - F_{Y_{ij}}(\mathrm{u}))\, d\, F_{X_{ij}}(\mathrm{u}) & z = z_{ij}, y = z_{i,j+1} \\ P\{X_i < X_k, 1 \leq k \leq m, k \neq i, X_i < t\} = & z = S, y = z_{i,1} \\ \quad = \int_0^t \left(\prod_{k=1, k \neq i}^{m} \left(1 - F_{X_k}(u)\right) \right) dF_{X_i}(u) & \\ P\{Y_F < t\} = F_{Y_F}(t) & z = F, y = S \\ 0 & w\ p.p. \end{cases}$$

gdzie X_i oznacza czas od wystąpienia stanu bezpieczeństwa S do momentu, kiedy rozpocznie się atak typu *i-tego*.

Dysponując jądrem semimarkowskim Q(t), łatwo wyznaczyć prawdopodobieństwa zmiany stanów procesu Z(t) (prawdopodobieństwa przejść włożonego łańcuch Markowa):

$p_{z,y} = \mathrm{P}\{\mathrm{Z}(t_{r+1}) = \mathrm{y} | \ \mathrm{Z}(t_r) = \mathrm{z},\}$ dla $z, y \in \boldsymbol{Z}$, korzystając z formuły:

$$p_{z,y} = Q_{z,y}(+\infty).$$

Zatem, otrzymujemy zależności:

$$p_{z,y} = \begin{cases} P\{X_{ij} > Y_{ij}\} = \int_0^{+\infty} (1 - F_{X_{ij}}(\mathrm{u}))\, d\, F_{Y_{ij}}(\mathrm{u}) & z = z_{ij}, y = S \\ P\{X_{ij} < Y_{ij}\} = \int_0^{+\infty} (1 - F_{Y_{ij}}(\mathrm{u}))\, d\, F_{X_{ij}}(\mathrm{u}) & z = z_{ij}, y = z_{i,j+1} \\ P\{X_i < X_k, 1 \le k \le m, k \ne i\} = & z = S, y = z_{i,1} \\ = \int_0^{+\infty} \left(\prod_{k=1, k \ne i}^{m} \left(1 - F_{X_k}(u)\right) \right) dF_{X_i}(u) & \\ P\{Y_F < t\} = F_{Y_F}(t) & z = F, y = S \\ 0 & w\ p.p. \end{cases}$$

Stochastyczny model ataku

Wykorzystując opracowany model można opisać metodę wyznaczania wartości wybranych wskaźników bezpieczeństwa systemu:

- ✓ Rozkład i oczekiwany czas do wystąpienia błędu bezpieczeństwa (stanu F) (mean time to security failure MTTSF);
- ✓ Graniczne (stacjonarne) prawdopodobieństwo przebywania w stanie:
  - ✓ Pełnego bezpieczeństwa (stan S);
  - ✓ Stanu realizacji niewykrytego ataku;
  - ✓ Docelowy stanu naruszenia bezpieczeństwa - błędu bezpieczeństwa (stan F).
- ✓ Czas utrzymywania się procesu w podzbiorze stanów A, począwszy od stanu z-tego oznaczymy jako η_z^A, a jej dystrybuantę jako $F_{\eta_z^A}$. Wyznacza się z układu równań:

$$F_{\eta_z^A}(t) = \sum_{y \in \mathbf{A}} \int_0^t F_{\eta_y^A}(t-u)\,dQ_{z,y}(u) + \sum_{w \in \bar{\mathbf{A}}} Q_{z,w}(t), \quad z \in \mathbf{A} \qquad (*)$$

lub po przekształceniu Laplace'a-Stieltjesa, układ równań algebraicznych:

$$F^*_{\eta_z^A}(s) = \sum_{y \in \mathbf{A}} F^*_{\eta_y^A}(s) Q^*_{z,y}(s) + \sum_{w \in \bar{\mathbf{A}}} Q^*_{z.w}(s), \quad z \in \mathbf{A} \qquad (**)$$

Stochastyczny model ataku

Problem wyznaczenia graniczne (stacjonarne) prawdopodobieństwo przebywania w stanie

- ✓ Przyjmujemy, że włożony łańcuch Markowa procesu Z(t) posiada następującą macierz prawdopodobieństw przejść w jednym kroku $\Pi(1) \equiv \Pi = [p_{z,y}]$
- ✓ Z poniższego układu równań, wyznaczmy stacjonarny rozkład prawdopodobieństwa włożonego łańcucha Markowa

$$\begin{cases} \pi = \pi \cdot \Pi \\ \sum_{i \in \mathbf{X}} \pi_i = 1 \end{cases} \Leftrightarrow \begin{cases} \pi(\Pi - I) = 0 \\ \sum_{i \in \mathbf{X}} \pi_i = 1 \end{cases}$$

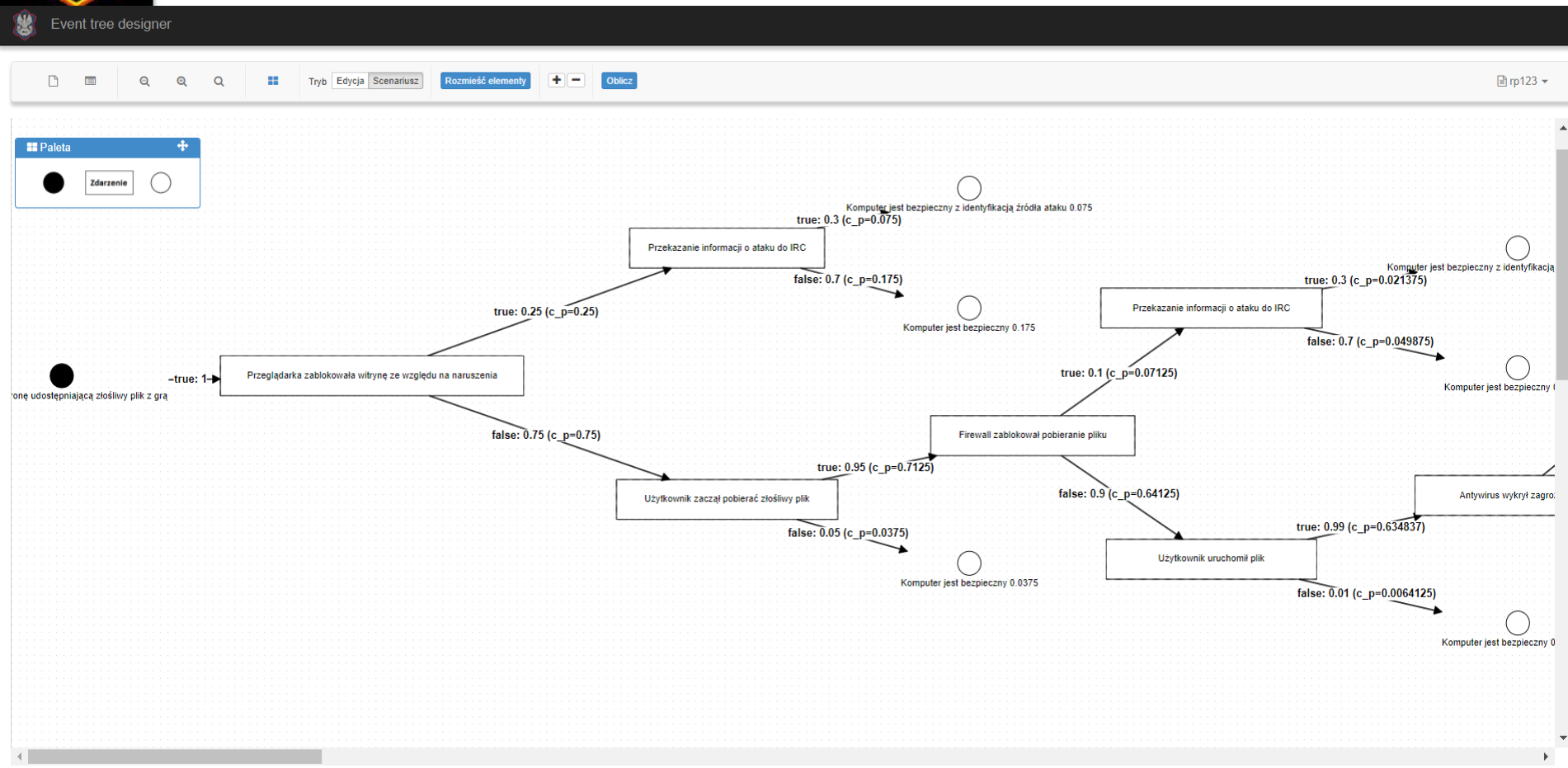
- ✓ Prawdopodobieństwa graniczne wyznaczany z zależności:

$$\lim_{t \to +\infty} P_z(t) = \frac{\pi_z \cdot E\{T_z\}}{T}$$

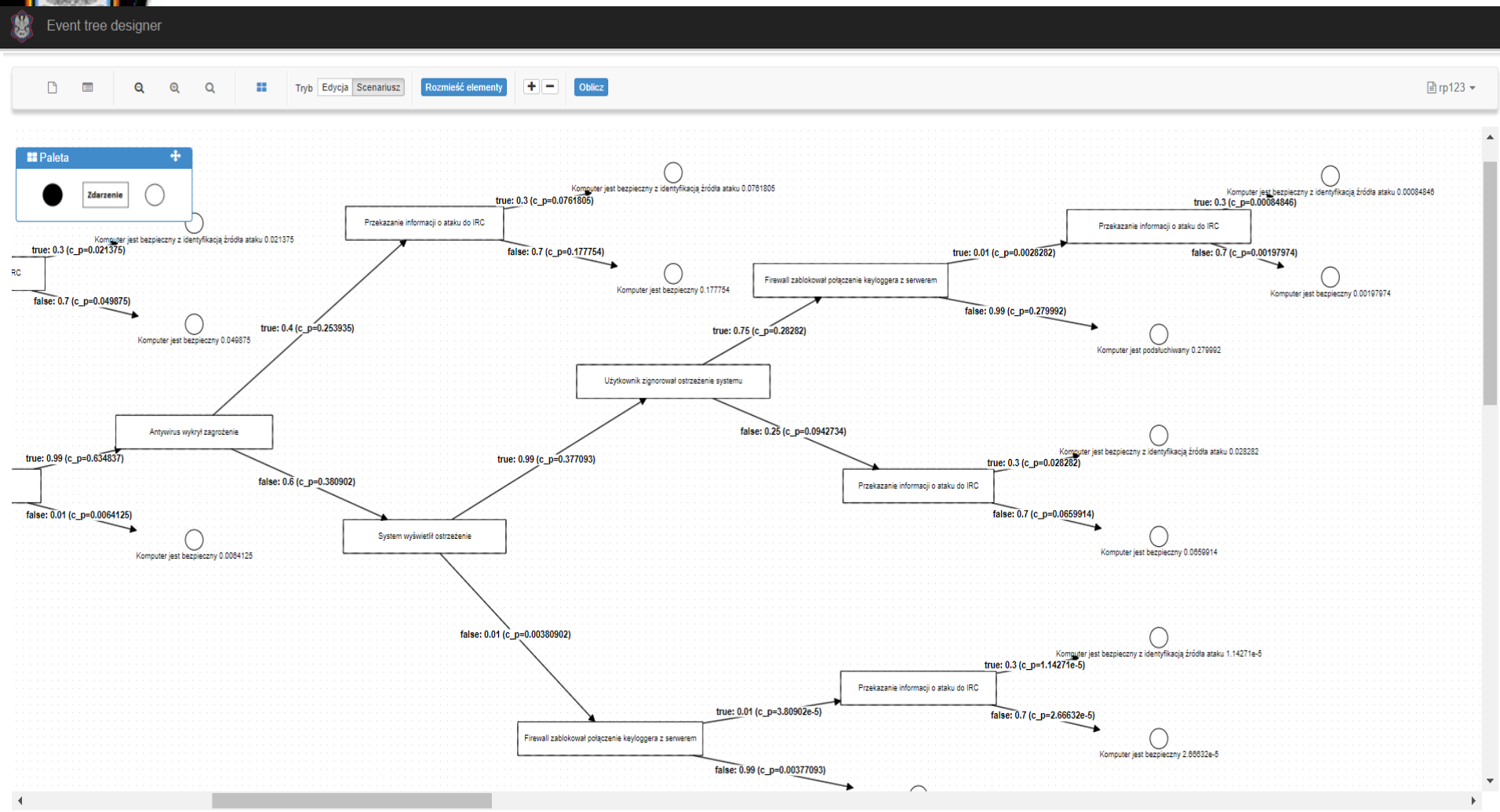
gdzie:

$$T = \sum_{z \in \mathbf{A}} E\{T_z\} \cdot \pi_z$$

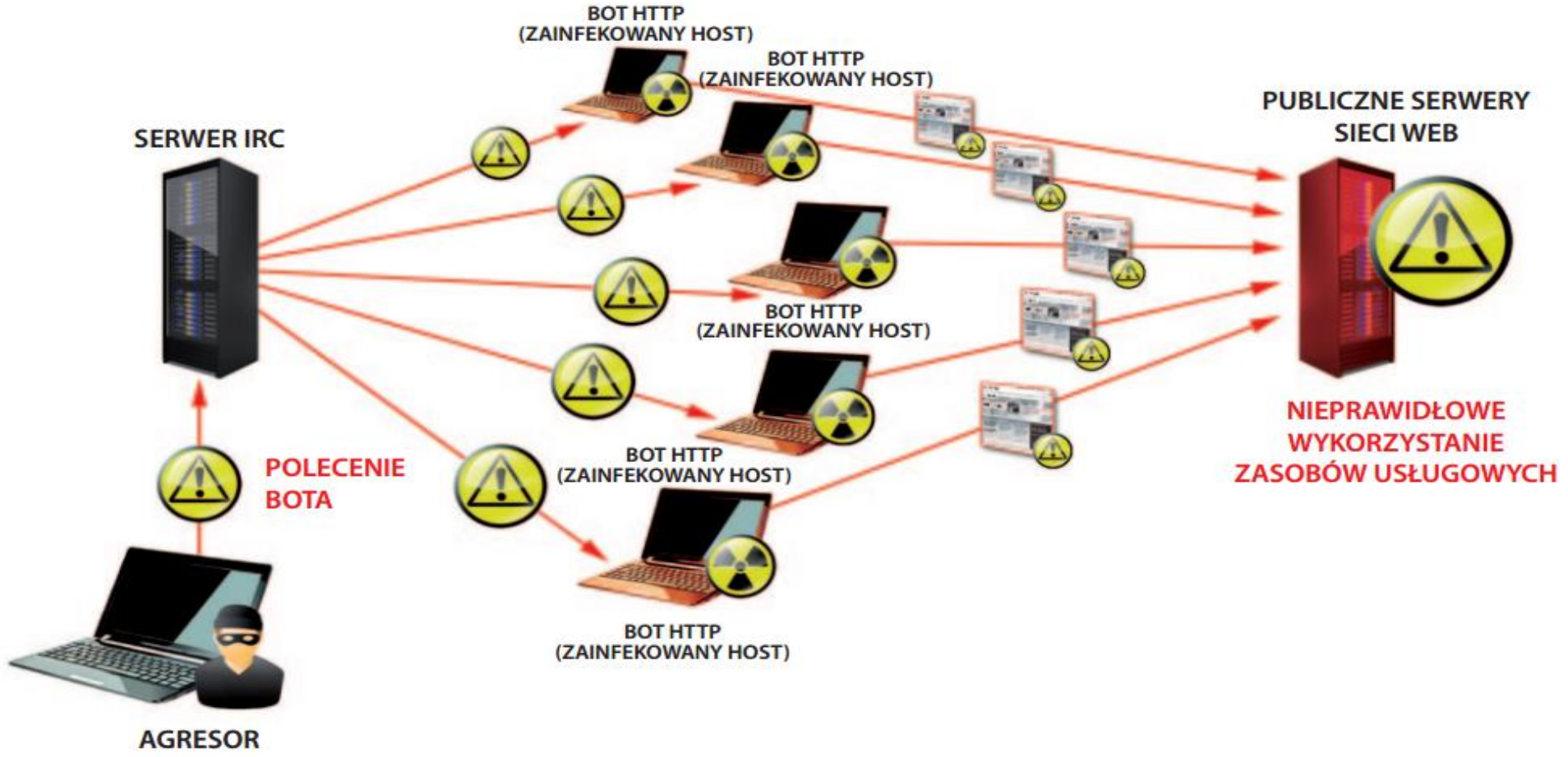
Drzewa zdarzeń



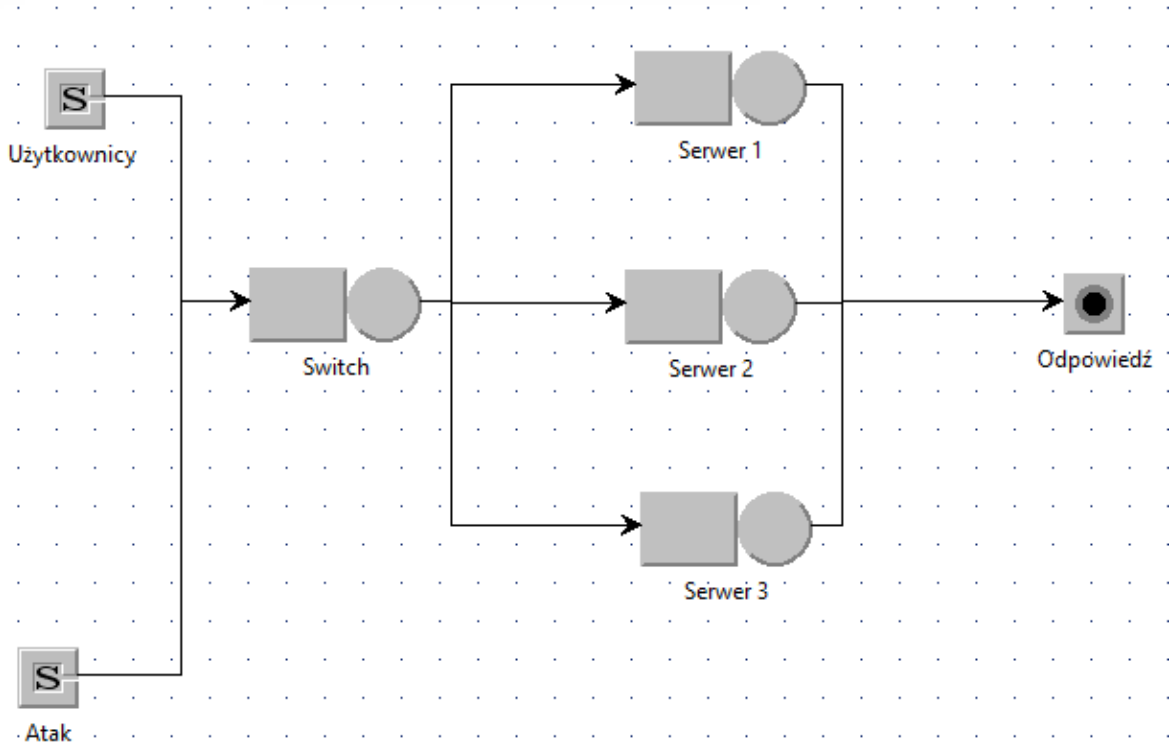
Drzewa zdarzeń



Ocena skutków ataku DoS



Model symulacyjny

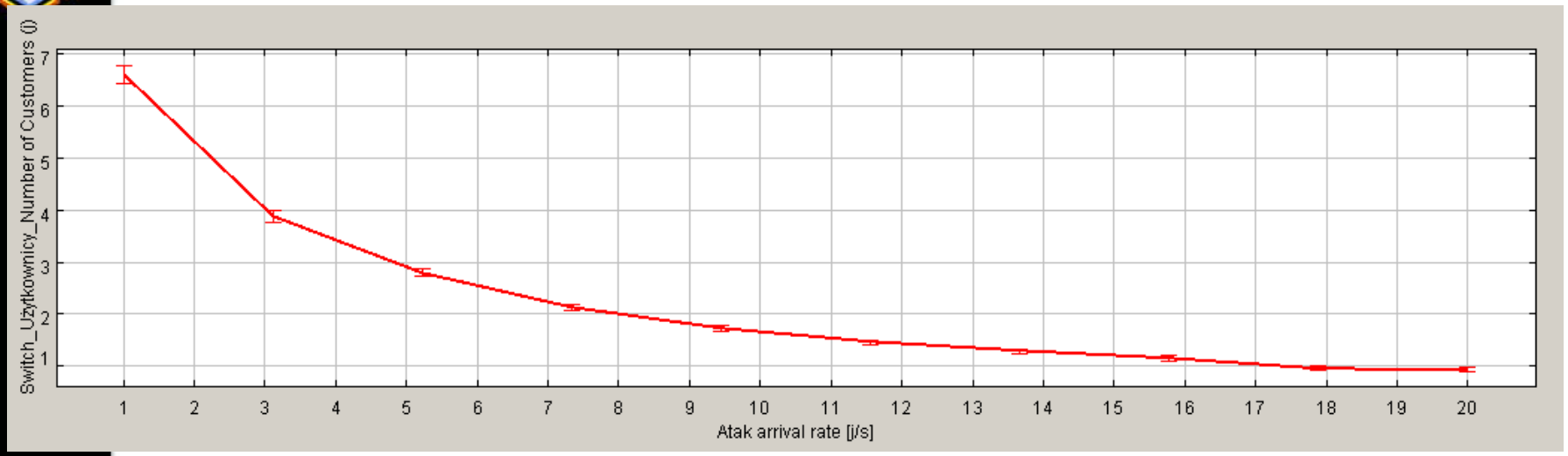


Badane charakterystyki:

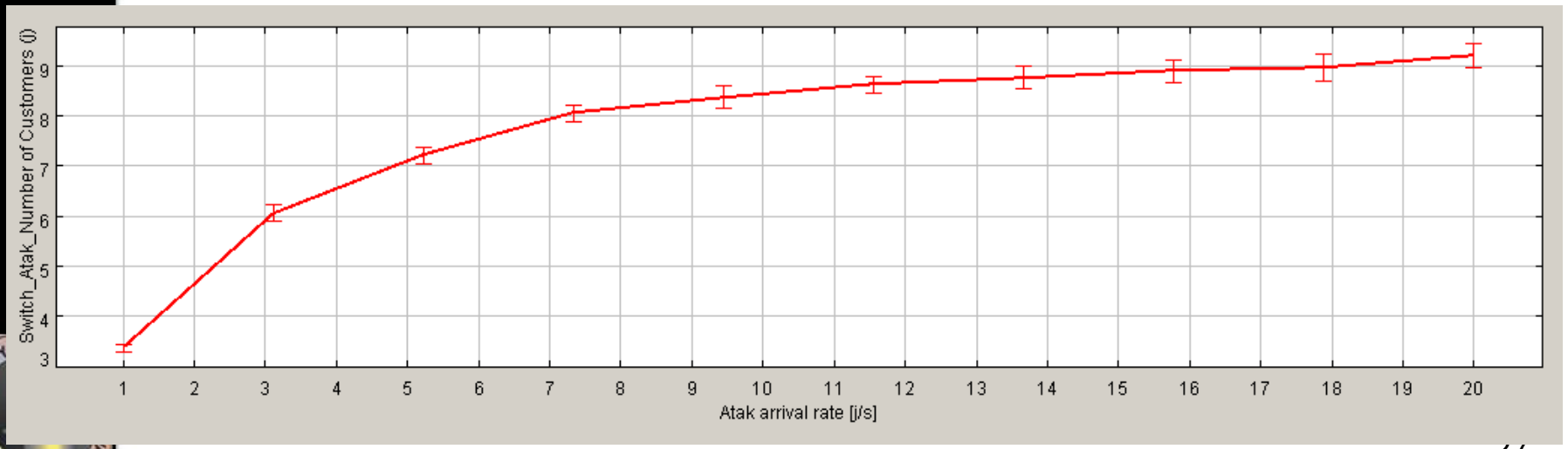
- ✓ liczba zgłoszeń obecnych w systemie
- ✓ intensywność odrzucania zgłoszeń
- ✓ wydajność systemu (obsługa zgłoszeń prawidłowych)

Wyniki eksperymentu

Liczba zgłoszeń (Number of Customers)



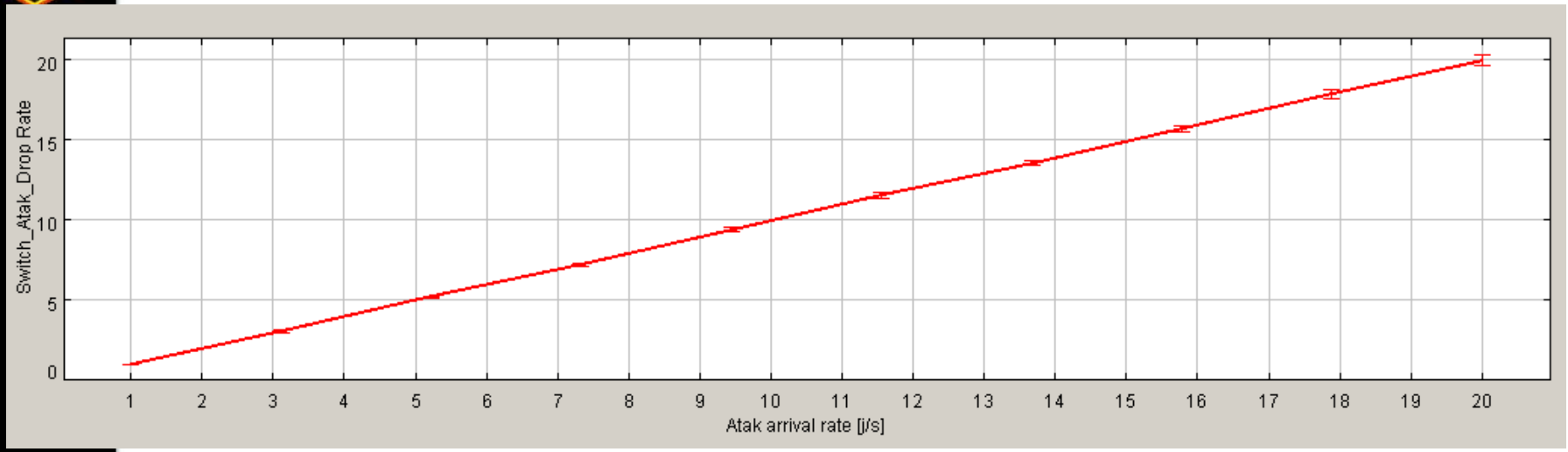
Switch - Użytkownicy



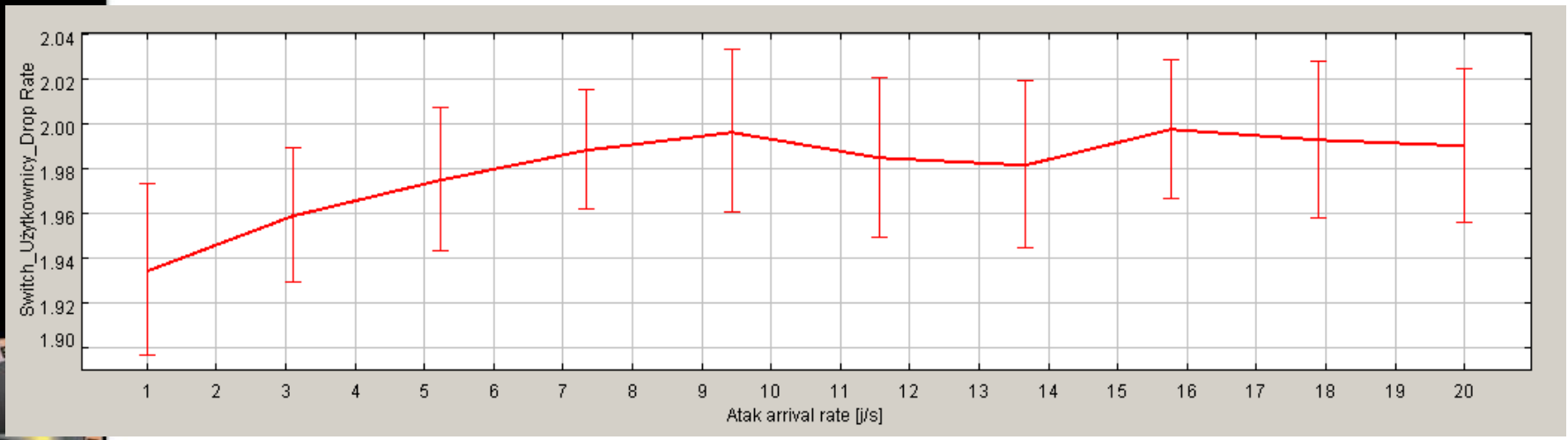
Switch - Atak

Wyniki eksperymentu

Intensywność odrzucania zgłoszeń (Drop Rate)



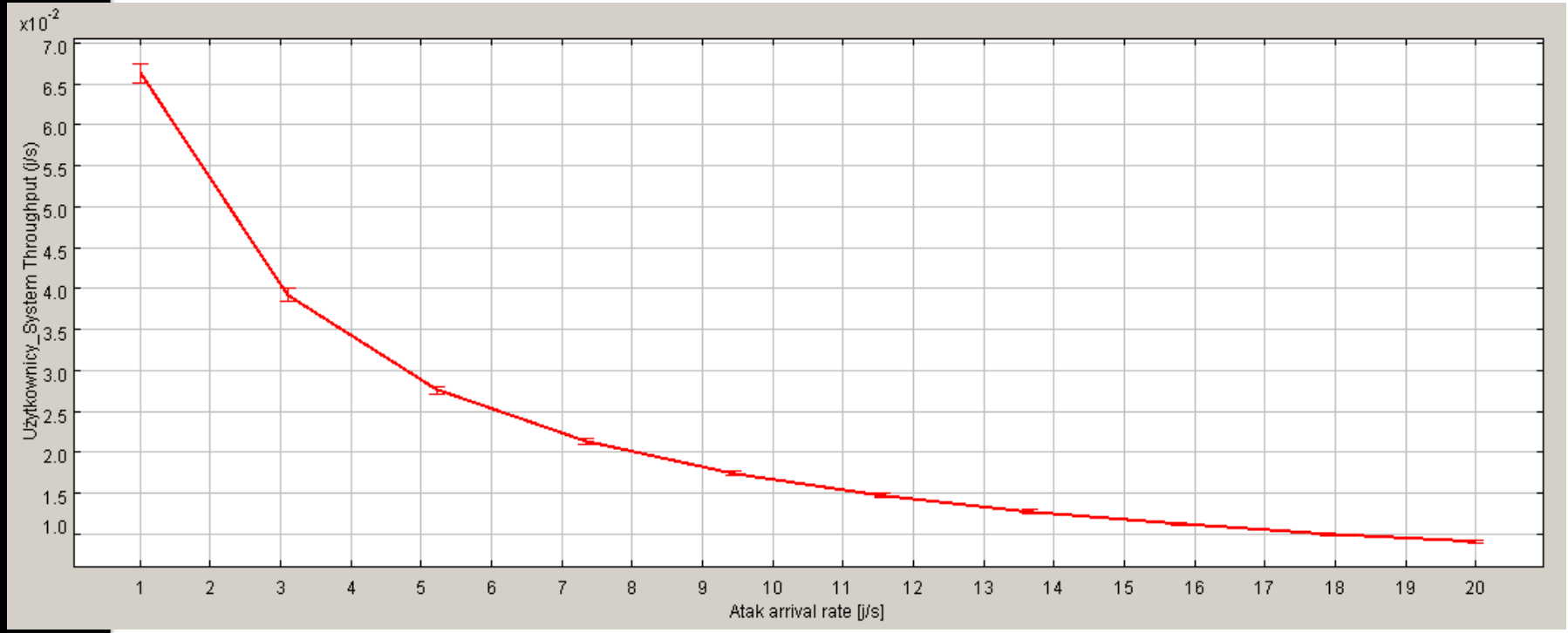
Switch - Atak



Switch - Użytkownicy

Wyniki eksperymentu

Wydajność systemu (System Throughput)

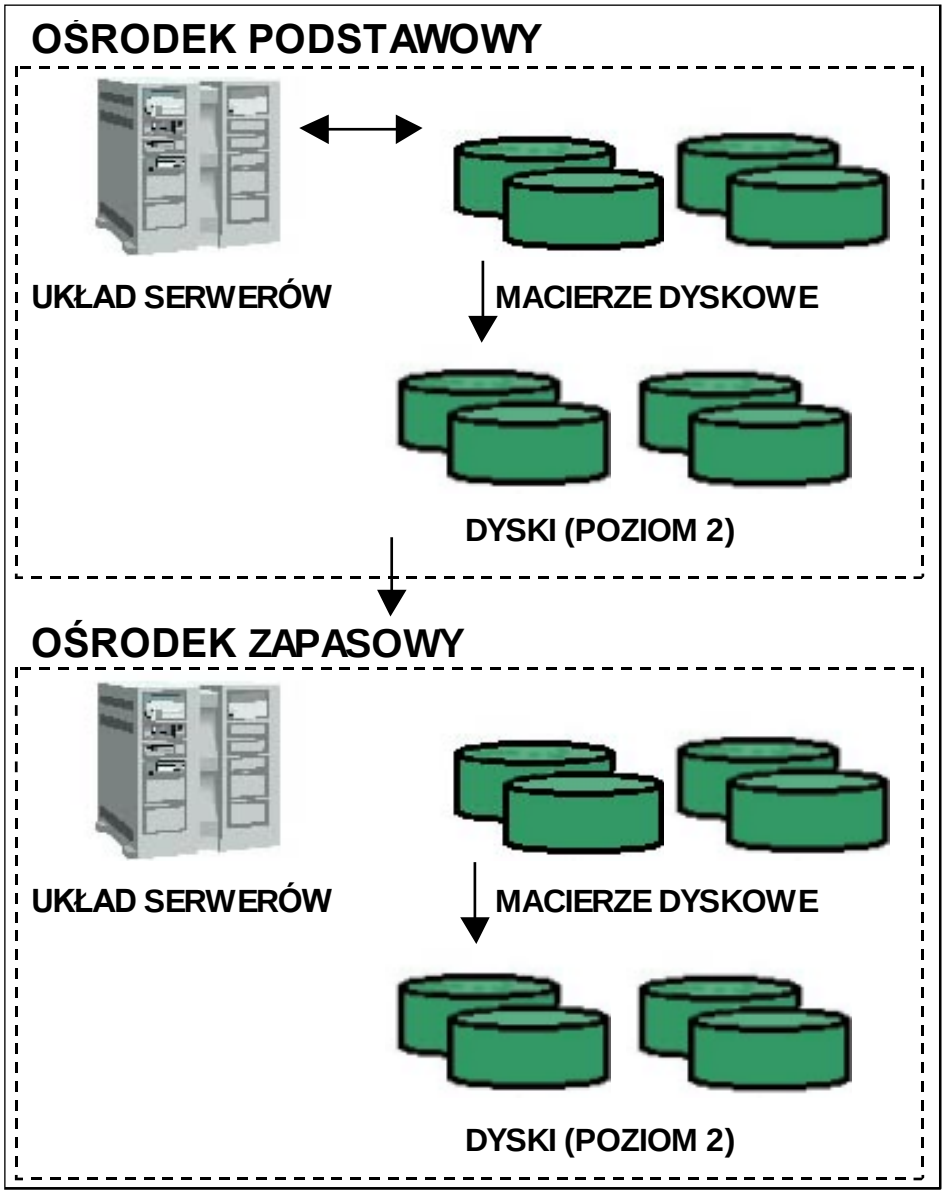


Użytkownicy

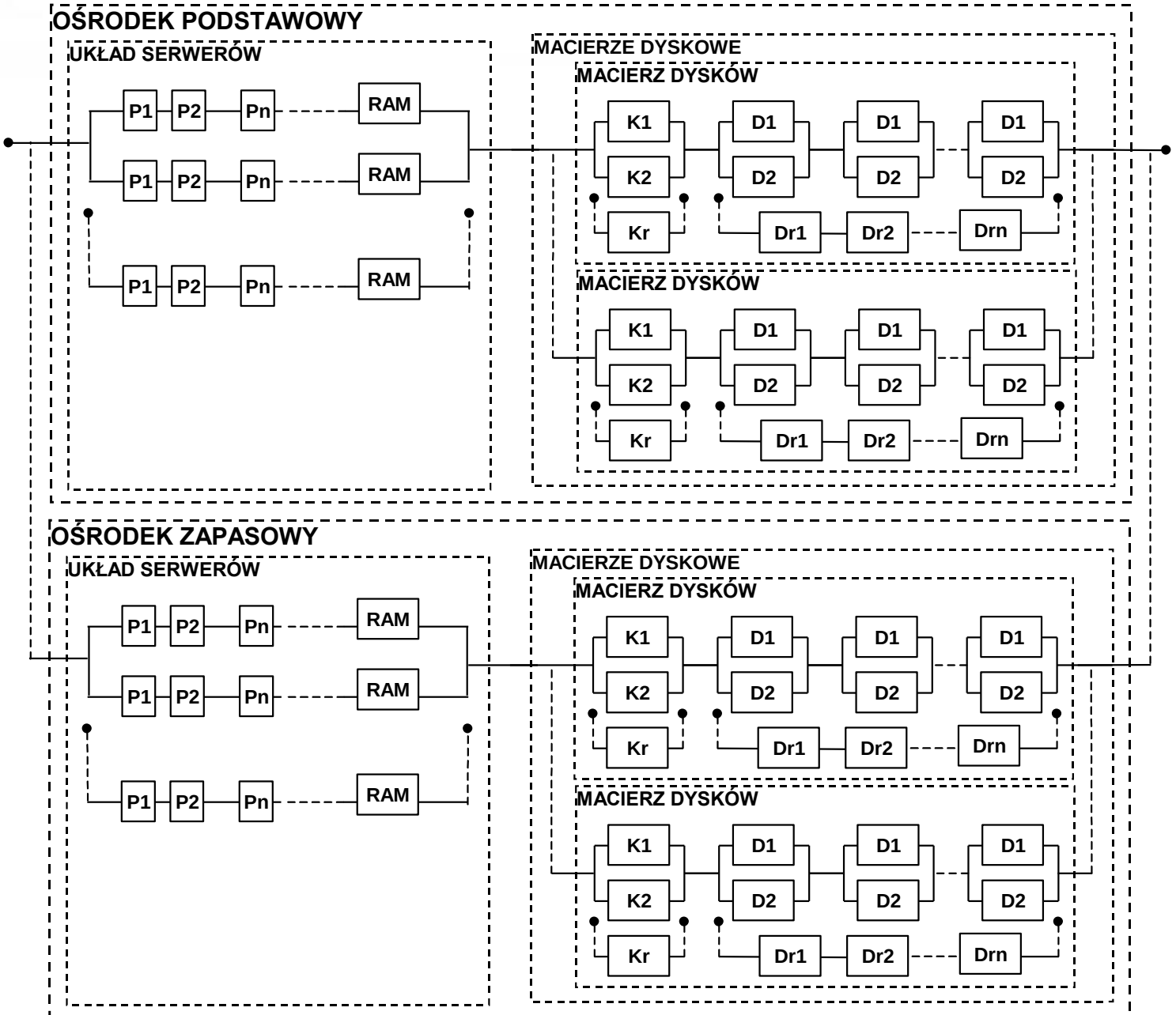
	1.000 j/s	2.000 j/s	3.000 j/s	4.000 j/s	5.000 j/s	6.000 j/s	7.000 j/s	8.000 j/s	9.000 j/s	10.000 j/s
Mean value (j/s)	0.066	0.039	0.028	0.021	0.017	0.015	0.013	0.011	0.010	0.009
Max (j/s) (Conf Int)	0.068	0.040	0.028	0.022	0.018	0.015	0.013	0.011	0.010	0.009
Min (j/s) (Conf Int)	0.065	0.038	0.027	0.021	0.017	0.015	0.013	0.011	0.010	0.009

Model niezawodnościowy systemu przetwarzania danych

- ✓ Zakładana struktura przykładowego systemu [Tyw]



Model niezawodnościowy systemu przetwarzania danych



Model niezawodnościowy systemu przetwarzania danych

- Przyjęte oznaczenia:
  - P1, P2, ...,Pn – procesory w serwerach,
  - RAM – pamięć operacyjna,
  - K1, K2 – kontrolery macierzy dyskowych,
  - Kr – kontroler rezerwowy (zapasowy),
  - D1, D2 – dyski twarde tworzące kopię lustrzaną,
  - Dr1, Dr2 – dyski twarde rezerwowe (zapasowe).

- Przy przyjętych założeniach i oznaczeniach wyznaczony zostanie stacjonarny współczynnik gotowości sytemu:

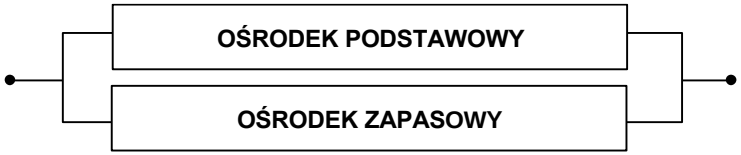
$$K_g = \lim_{t \to +\infty} k_g(t) = \lim_{t \to +\infty} P\{Y(t) = 1\}$$

gdzie:

$$Y(t) = \begin{cases} 1 & system\ sprawny \\ 0 & system\ niesprawny \end{cases}$$

Model niezawodnościowy systemu przetwarzania danych

✓ Z przyjętych założeń wynika, że system ma strukturę równoległą:

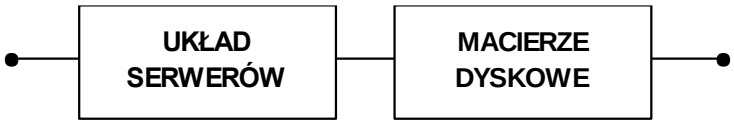


a jego współczynnik gotowości można wyznaczyć z zależności:

$$K_g = 1 - (1 - K_{gP})(1 - K_{gZ})$$

gdzie:
K_{gP}- współczynnik gotowości ośrodka podstawowego;
K_{gZ}- współczynnik gotowości ośrodka zapasowego.

<u>Wyznaczanie stacjonarnego współczynnika gotowości ośrodka podstawowego</u>
(zapasowego – identyczna struktura i założenia działania)
Struktura niezawodnościowa ośrodka obliczeniowego:



Model niezawodnościowy systemu przetwarzania danych

- ✓ Zatem, jego wskaźnik gotowości określa następująca zależność:

$$K_{gP} = K_{gS} \cdot K_{gM}$$

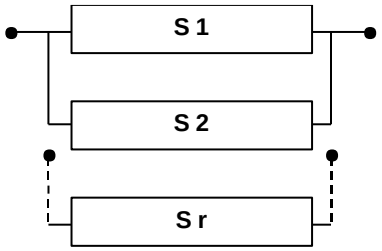
gdzie:

K_{gS}- stacjonarny współczynnik gotowości układu serwerów;

K_{gM}- współczynnik gotowości macierzy dyskowych.

<u>Stacjonarny współczynnik gotowości układu serwerów</u>

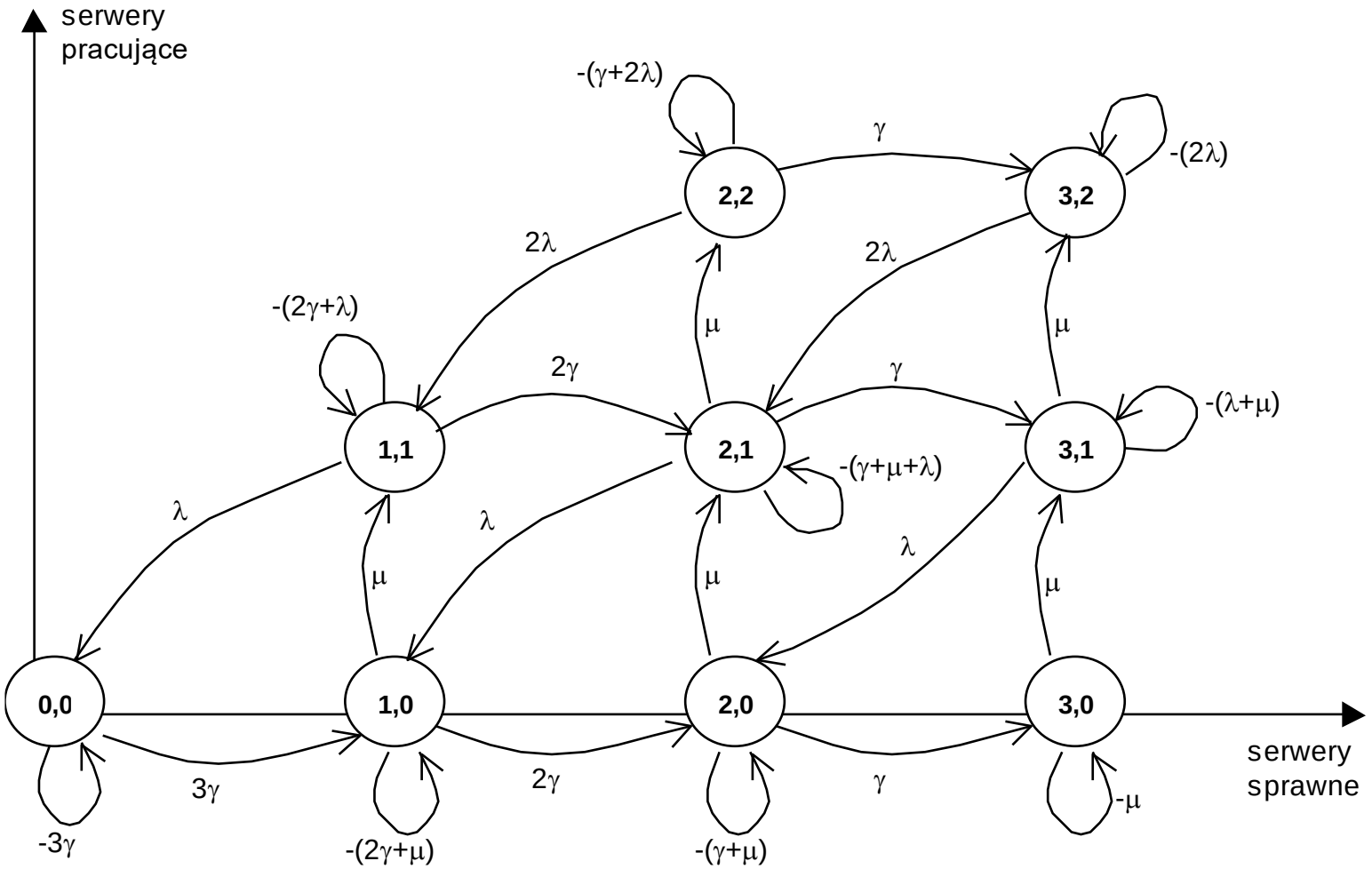
- ✓ Struktura niezawodnościowa układu serwerów:



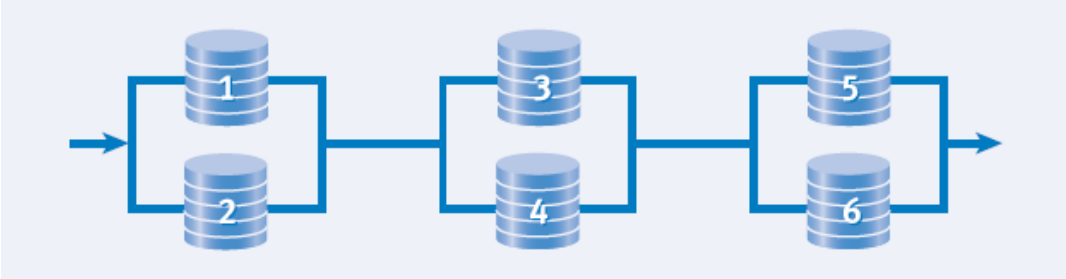
- ✓ W celu wyznaczenia współczynnika gotowości, przyjmuje się następujące założenia:

Stacjonarny współczynnik gotowości układu serwerów

- Graficzna reprezentacja procesów Markowa dla n_S = 3 oraz k_{Smax} = 2 przedstawiona jest na rysunku:



- ✓ W macierzy RAID – 1 pliki dyski ustawiane są w pary, a każdy plik jest duplikowane i zapisywany na obu dyskach wybranej pary.
- ✓ W konfiguracji RAID-1 n HDD dzielonych jest na n/2 par. Utrata danych następuję wówczas, gdy uszkodzeniu ulegną oba dyski w jednej z par.
- ✓ Zatem struktura niezawodnościowa konfiguracji RAID-1 dla n=6 ma postać:



a funkcja niezawodności dla dowolnego parzystego n ma postać:

$$R_{RAID-1}(\mathrm{t}) = \prod_{j=1}^{[\frac{n}{2}]}(1-(1-R_{HDD_{j1}}(t))(1-R_{HDD_{j2}}(t)))$$

gdzie: $R_{HDD_{jk}}(t), k = 1{,}2$ jest funkcją niezawodności elementu k-tego j-tej pary dysków.

Dla danych: $n = 14, t = 3\ lata, R_{HDD_i}(3) = 0.9$ otrzymujemy następujący wynik:

Metody ilościowe stosowane do wykrywana zagrożeń cybernetycznych

[Garcia]

- Detection Algorithms
  - Instance-based learning
    - k-nearest neighbor [35]
  - Supervised
    - HMM [37]
    - Bayesian Statistics [33][34]
    - Artificial Neural Networks
    - SVM
    - Decision Trees [34]
  - Semi-supervised
    - EM
    - Co-training
  - Unsupervised
    - HMM
    - Clustering [30][27][28][31][35][13]
    - SOM
    - ART
  - Signal Processing
    - Autocorrelation [27b]
    - CUSUM [31]
    - SPRT [27]
  - Heuristic Rules [28][27][30][10][32][34][29][36][31][33][35][37][13]

Bibliografia

- [Alhazmi05] O. H. Alhazmi and Y. K. Malaiya, Modeling the Vulnerability Discovery Process, Proceedings of the 16th IEEE International Symposium on Software Reliability Engineering (ISSRE'05)
- [Alhazmi06] Alhazmi O. H., Malaiya Y. K., Prediction Capabilities of Vulnerability Discovery Models, Proc. Reliability and Maintainability Symposium, January 2006
- [Azg] Almasizadeh J., Azgomi M. A., A stochastic model of attack process for the evaluation of security metrics, Computer Networks 57 (2013) 2159–2180
- [Biał] Białas Andrzej – Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2006
- [Das] Saini Das , Arunabha Mukhopadhyay, Girja.K. Shukla - i-HOPE Framework for Predicting Cyber Breaches: A Logit Approach, 2013 46th Hawaii International Conference on System Sciences
- [Garcia] Sebastián García, Alejandro Zunino and Marcelo Campo - Survey on network-based botnet detection methods, SECURITY AND COMMUNICATION NETWORKS (2013)
- [Lid] Liderman Krzysztof – Analiza ryzyka i ochrona informacji w systemach komputerowych, Wydawnictwo naukowe PWN, Warszawa 2008
- [Younis] YounisA.A., Joh H., and Yashwant K. Malaiya Y.K., Modeling Learningless Vulnerability Discovery using a Folded Distribution, Int'l Conf. Security and Management, SAM'11