MODEL I METODA PROGNOZOWANIA PODATNOŚCI OPROGRAMOWANIA NA ZAGROŻENIA W CYBERPRZESTRZENI

mjr mgr inż. Artur STACHURSKI

Z przeprowadzonych analiz statystycznych podatności wynika, iż podatności występują niemal w każdym dostępnym powszechnie oprogramowaniu. Jednocześnie, pomimo posiadania szerokiego zakresu zdolności do identyfikacji podatności w oprogramowaniu od strony technicznej, ustalenie zależności analitycznych nie jest procesem trywialnym. W związku z tym zadanie rozwiązania racjonalnego zapewnienia bezpieczeństwa oprogramowania implikuje konieczność posiadania informacji prognostycznej dotyczącej potencjalnych podatności.

Niniejsza praca przedstawia opis autorskich modeli i metod probabilistycznych w procesie prognozowania podatności oprogramowania, przy wykorzystaniu wybranych własności łańcucha Markowa. Zaproponowane modele i metody przeznaczone są do analiz oprogramowania dedykowanego, tzn. takiego, którego projekt i implementacja zostały zlecone przez dany podmiot innemu podmiotowi i nie jest przewidziana jego dystrybucja dla odbiorców z zewnątrz, na bazie rzeczywistych danych pozyskanych podczas testów bezpieczeństwa. W rezultacie możliwe jest oszacowanie i ocena niżej wymienionych właściwości:

- Poziom bezpieczeństwa oprogramowania;
- Intensywność wykrywania krytycznych podatności oprogramowania;
- Skuteczność zastosowanych działań profilaktyczno-naprawczych.

Jako rozszerzenie zdolności zaproponowanych modeli matematycznych, w kontekście przyporządkowania nowo-wykrytych podatności do zdefiniowanych kategorii podatności, zaproponowano rozwiązanie bazujące na mechanizmach uczenia maszynowego. Wykorzystano kilka wybranych modeli uczenia maszynowego, które zostały wytrenowane przy użyciu danych z referencyjnej bazy danych podatności NVD (*National Vulnerability Database* – zarządzanej przez *NIST*), celem identyfikacji optymalnego rozwiązania.

Zastosowanie zaproponowanych modeli matematycznych w procesie wnioskowania ma na celu usprawnić jakościową i ilościową analizę zgromadzonych danych, a jednocześnie pozwoli na bardziej kompleksową i dokładniejszą ocenę poziomu bezpieczeństwa oprogramowania, wyznaczając tym samym ocenę możliwych przejść oprogramowania ze stanu bezpiecznego w stan podatny.