Rank thresholds in classifier ensembles in medical diagnosis

Progowanie rang dla zespołów klasyfikatorów w diagnostyce medycznej

K. ANTCZAK
karol.antczak@wat.edu.pl

Military University of Technology, Faculty of Cybernetics
Institute of Computer and Information Systems
Kaliskiego Str. 2, 00-908 Warsaw, Poland

Classification methods have multiple applications, with medical diagnosis being one of the most common. A powerful way to improve classification quality is to combine single classifiers into an ensemble. One of the approaches for creating such ensembles is to combine class rankings from base classifiers. In this paper, two rank-based ensemble methods are studied: Highest Rank and Borda Count. Furthermore, the effect of applying class rank threshold to these methods is analyzed. We performed tests using real-life medical data. It turns out that specificity of data domain can affect classification quality depending on classifier type.

Keywords: medical diagnostics, classifier ensemble, rank threshold.

Metody klasyfikacji mają wiele zastosowań, z których jednym z częściej spotykanych jest diagnostyka medyczna. Jakość klasyfikacji można w znaczący sposób podnieść, tworząc zespoły klasyfikatorów. Jedną z metod tworzenia takich zespołów jest łączenie rankingów generowanych przez klasyfikatory bazowe. W niniejszej pracy przeanalizowano dwie metody łączenia klasyfikatorów bazujące na rankingach: Najwyższej Rangi oraz Głosowanie Bordy. Dodatkowo zbadano wpływ progowania rankingu na jakość klasyfikacji. Testy przeprowadzono z użyciem rzeczywistych danych medycznych. Wykazano przy tym, że specyfika danych medycznych może wpłynąć na jakość klasyfikacji w zależności od typu klasyfikatora.

Słowa kluczowe: diagnostyka medyczna, łączenie klasyfikatorów, progowanie rankingu.

Comuter Science and Mathematical Modelling, ISSN 2450-0054, No. 3, 5–12 (2016)

Choosing the optimal strategy for information security in a business organization

Metoda symulacyjna wyboru optymalnej strategii bezpieczeństwa informacyjnego w organizacji biznesowej

A. CHOJNACKI, G. PIENIĄŻEK
andrzej.chojnacki@wat.edu.pl, grzegorz.pieniazek@gmail

Military University of Technology, Faculty of Cybernetics,
Institute of Computer and Information Systems
Kaliskiego Str. 2, 00-908 Warsaw, Poland

The paper describes the method of choosing the optimal strategy to implement security measures in a business organization. Strategies are categorized depending on time horizons, the history of threats and implemented security measures. Next, the method of choosing the optimal strategy for a business organization in a given context is outlined. Then this method is used to select the optimal strategy in a particular business context. The method is based on a deterministic time-based information security model, which was extended to a random model. With this simulation method, an organization can choose a strategy to implement security measures that best suits its needs. It is important for organizations to conduct an analysis of costs and threats in order to select appropriate safeguards.

Keywords: information security, stochastic model, simulation.

W artykule opisano strategie wdrażania zabezpieczeń w organizacji biznesowej. Strategie są sklasyfikowane w grupy według zależności od historii występowania zagrożeń oraz zależności od historii wdrażanych zabezpieczeń. Następnie przedstawiona jest metoda wyboru optymalnej strategii dla organizacji biznesowej, przy ustalonym kontekście. W kolejnym kroku wprowadzona metoda jest użyta do wyboru optymalnej strategii w przykładowym przypadku biznesowym. Metoda bazuje na deterministycznym, czasowym modelu bezpieczeństwa informacyjnego, który został rozszerzony do modelu losowego. Dzięki metodzie symulacyjnej organizacja może wybrać najlepszą, dla siebie, strategię wdrażania zabezpieczeń. Jest to istotne we współczesnych organizacjach, aby przeprowadzić analizę kosztów i ryzyka, w celu doboru odpowiednich zabezpieczeń.

Słowa kluczowe: bezpieczeństwo informacyjne, symulacja, strategia.

Introducing Enterprise Architecture Framework in Statistics Poland

Model procesu ubywania w sytuacji istnienia obiektów pozornych

J. DYGASZEWICZ[*], B. SZAFRAŃSKI[**]

j.dygaszewicz@stat.gov.pl
boleslaw.szafranski@wat.edu.pl

[*]Central Statistical Office of Poland
Al. Niepodległości 208, 00-925 Warsaw, Poland

[**]Military University of Technology, Faculty of Cybernetics
Kaliskiego Str. 2, 00-908 Warsaw, Poland

Article is devoted to the modernization of the statistical production process. The starting point for formulating the principles and methods of the modernization is to establish a framework architecture. An in-depth analysis of all relevant aspects arising from the holistic approach to the production of statistics is essential to extract the key business issues. Business needs are the foundation for the formulation of a coherent and transparent guidelines, demands, legal and technical requirements, both domestic and international which are the basis for the construction of the enterprise architecture framework and the development of solutions used to carry out the tasks of public statistics. The process of constructing architectural framework requires the use of models and methods used in scientific research, in particular arising from the achievements of enterprise architecture and modeling tools for object-oriented computing.

Keywords: enterprise architecture framework, statistics survey, GSBPM, TOGAF.

Artykuł poświęcony jest modernizacji procesu produkcji statystyki publicznej. Punktem wyjścia do formułowania zasad i metod modernizacji jest ustanowienie ram architektonicznych. Dogłębna analiza wszystkich istotnych aspektów wynikających z holistycznego podejścia do zagadnienia produkcji statystycznej jest podstawą do wyodrębnienia kluczowych zagadnień biznesowych. Potrzeby biznesowe stają się fundamentem do sformułowania spójnych i przejrzystych wytycznych, postulatów, wymagań prawnych i technicznych, zarówno krajowych, jak i międzynarodowych stanowiących podstawę do budowy ram architektonicznych oraz rozwoju rozwiązań informatycznych wykorzystywanych do realizacji zadań statystyki publicznej. Proces konstruowania ram architektonicznych wymaga zastosowania modeli i metod stosowanych w badaniach naukowych, w tym zwłaszcza wynikających z dorobku architektury korporacyjnej oraz modelowania obiektowego narzędziami informatyki.

Słowa kluczowe: ramy architektury korporacyjnej, badania statystyczne, GSBPM, TOGAF.

A concept of standard-based vulnerability management automation for IT systems

Oparta na standardach koncepcja zarządzania podatnościami systemów teleinformatycznych na zagrożenia

R. KASPRZYK, A. STACHURSKI
rkasprzyk@wat.edu.pl

Institute of Computer and Information Systems
Faculty of Cybernetics, Military University of Technology
Kaliskiego Str. 2, 00-908 Warsaw

The paper focuses on the attempt to show a way of automating IT vulnerability management across enterprise systems with the use of the Security Content Automation Protocol. SCAP offers a set of components which provide, among others, adjustable security checklists, standardised dictionaries of security vulnerabilities and vulnerability scoring methods that may prove valuable for organisations in terms of security analysis activities and quantitative risk assessment.

Keywords: vulnerabilities, SCAP, security.

Celem artykułu jest przedstawienie próby automatyzacji zarządzania podatnościami systemów teleinformatycznych przy zastosowaniu grupy standardów wchodzącej w skład SCAP (*The Security Content Automation Protocol*). Cel ten może zostać osiągnięty między innymi poprzez zdefiniowanie standardowych formatów nazw i słowników artefaktów związanych z bezpieczeństwem systemów teleinformatycznych, tworzenie kwestionariuszy pozwalających zarówno na manualną i programową ewaluację zgodności z założoną polityką bezpieczeństwa, jak i na badania charakterystyk konkretnych podatności. Działania te mogą wspomóc czynności związane ze szczegółową analizą bezpieczeństwa systemów IT, jak również z szacowaniem ryzyka potencjalnego ataku cybernetycznego.

Słowa kluczowe: podatność na cyberzagrożenia, SCAP, bezpieczeństwo teleinformatyczne.

Comuter Science and Mathematical Modelling, ISSN 2450-0054, No. 3, 33–38 (2016)

Profile Cloning Detection in Online Social Networks

Wykrywanie klonowania profili w internetowych sieciach społecznych

M. ZABIELSKI, Z. TARAPATA, R. KASPRZYK, K. SZKÓŁKA

mzabielski@wat.edu.pl, ztarapata@wat.edu.pl, rkasprzyk@wat.edu.pl, kszkolka@wat.edu.pl

Military University of Technology, Faculty of Cybernetics,
Institute of Computer and Information Systems
Kaliskiego Str. 2, 00-908 Warsaw, Poland

Due to the emergence of online social networks, the importance of privacy on the Internet has vitally increased. Thus, it is important to develop mechanisms that will prevent our hidden personal data from unauthorized access and use. In this paper an attempt was made to present a concept of profile cloning detection in Online Social Networks (OSN) using Graph and Network Theory. Compering values of attributes of users' personal profiles and analysing structural similarity of networks, we identify attackers which steal users' identity.

Keywords: profile cloning detection, online social networks, violations of privacy.

Zagadnienie ochrony prywatności w Internecie istnieje od dosyć dawna, jednakże wraz z pojawieniem się internetowych sieci społecznych znaczenie tego tematu wzrosło drastycznie. Wynika to z faktu, iż sieci te są źródłem istotnych informacji osobowych powiązanych z konkretnym człowiekiem, które w dość prosty sposób są możliwe do wprowadzenia do informacji publicznej. Ważną kwestią jest zatem opracowanie mechanizmu, który uniemożliwi osobom niepowołanym wykrycie danych osobowych ukrytych przed dostępem publicznym. W pracy podjęto próbę przedstawienia koncepcji mechanizmu wykrywania klonowania profilu użytkownika w Internetowej Sieci Społecznej z wykorzystaniem teorii grafów i sieci. Analizując podobieństwo strukturalne sieci wraz z atrybutami opisującymi osobę w niej, jesteśmy w stanie znaleźć osoby próbujące ukraść naszą tożsamość.

Słowa kluczowe: wykrywanie klonowania profilu, internetowe sieci społeczne, naruszenie prywatności danych.

Comuter Science and Mathematical Modelling, ISSN 2450-0054, No. 3, 39–46 (2016)