HUNGARIAN JOURNAL
OF INDUSTRY AND CHEMISTRY
VESZPRÉM
Vol. 42(2) pp. 79–84 (2014)

CHALLENGES OF ENTERPRISE POLICY COMPLIANCE WITH SMARTPHONE ENABLEMENT OR AN ALTERNATIVE SOLUTION BASED ON BEHAVIOUR-BASED USER IDENTIFICATION

SÁNDOR DOBOS✉ AND ATTILA KOVÁCS

Department of Information Technology, ELTE University Budapest, Budapest, 1117, HUNGARY
✉Email: sandor.dobos@hu.ibm.com

Current trends show the intense growth in the role and importance of mobile technology (smartphones, tablets, etc.) in business due to economic, social and technological reasons. The social element drives a powerful convenience expectation called "Bring Your Own Device" (BYOD) for taking notes and accessing internal and external network resources. Apparently, the future is leading toward a more extensive enablement of smartphones and tablets with their enterprise applications. Internal security standards along with applicable regulatory ones to achieve 'policy enforcement' as types of solutions and controls; however, this allows for merely one aspect of compliance. An alternative solution could be behaviour-based analysis to identify the user, attacker or even a malicious program accessing resources on phone or internal networks. Complex networks can be defined by graphs, such as connections to resources on smartphones and serve as a blueprint. In case the motif is different from the user's actual behaviour, the company can initiate specific actions to avoid potential security violations. This document reviews the IT security challenges related to smartphones as well as the concept of graph-based user identification. The challenges of the latter are the identification of motif, selection of search algorithm and defining rules for what is considered a good or bad behaviour.

Keywords: mobile device security, "Bring Your Own Device" (BYOD) management, secure data communication, behaviour-based identification of threat, graph-based user identification

Introduction

Enterprise policy enforcement with current mobile technology management tools (Mobile Device Management (MDM), virus detection, and other necessary modules) ensure only the compliance of piece of equipment. Within enterprise, MDM Servers initiate the compliant actions, if the smartphone client fails the access privilege is taken away; however, this has an immediate impact on revenue through operational efficiency affecting the business. The enterprise compliance of the smartphone device is only a validated response, which can be altered by understanding the mobile technology, such as the application structures or the way MDM technology works. Hackers are heavily attacking smart devices with malicious software (Malware). These can be viruses, spyware, adware, and other types of attacks. A specific example is the "`Obad.a` Trojan", which is now being distributed *via* mobile botnets. The trojans are occupying a larger space and becoming more complex, which shows the need for IT security to find new ways to detect them.

The secure enterprise environment is crucial for organizations to ensure the business strategy and continuity of operation, irrespective of its environment being production, service delivery, or customer support related. Companies are following the trend to ensure efficiency and simplify service accessibility for their customers, business partners or employees. It is an essential element of the IT security strategy to be aligned with the business strategy due to (i) the intense growth of mobile technology and (ii) pressure from enterprise that has transformed business operations.

Forrester Research from the Q2 Foresights Security Survey shows (*Fig.1*) that mobile security is of primary concern amongst enterprise leaders. CEOs are concerned about the risk of data loss, particularly due to device loss or theft. Another worry regards data protection or data leak prevention usually in connection with data related to finance and innovation.

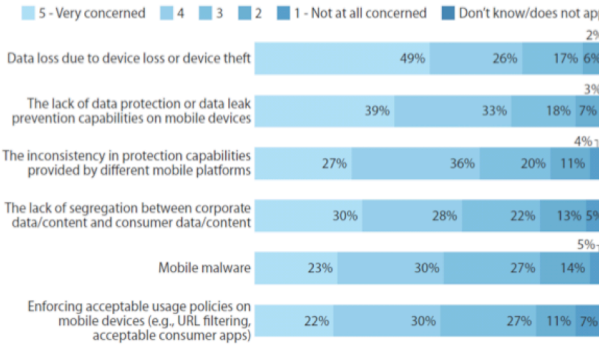

Figure 1: Degree of concern of CEOs from Forrester Research, Foresights Security Survey

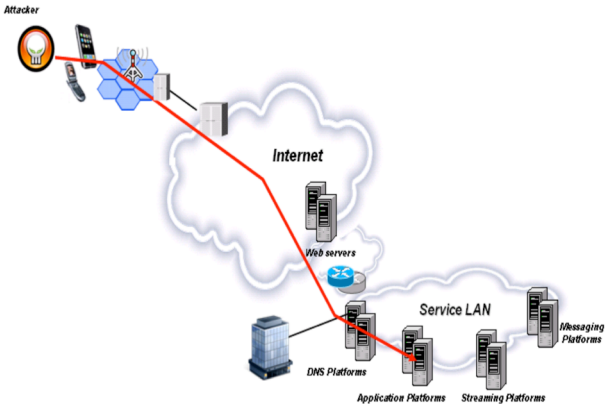

Figure 2: Graphical illustration of mobile phone technology security threats

Current Challenges

Within today's economic environment, profit-driven organizations are challenged from revenue, growth or profit target perspectives. In order to meet such expectations, organizations are under high pressure to offer innovative products (services) within newly identified channels and more accessible yet-to-be-penetrated markets to a demanding customer base, especially in the area of providing smartphone solutions. On the other hand, regulatory bodies are alarmed at mobile enablement and organizations in general striving to protect critical financial systems better, in particular via identity and access management. At the same time, organizations need to maintain operational resiliency and perform risk management assessments as an integrated part of day-to-day operations. The cost perspective is an important factor for customers facing the task of achieving a lower total cost of ownership (TCO) although, by this shift in paradigm, they move from reactive protection to proactive value creation mode.

The alignment of the current IT strategy to business strategy is a challenge for corporations as IT is a service provider within an enterprise also offering business enablement leads. Companies need to manage security policy at the corporate level, assess the security health of the heterogeneous IT environment, monitor the security weakness(es) in processes and systems and, of course, meet the plethora of banking laws, regulations and standards including SOX, BASEL III, GLBA, and PCI compliance.

With the adaptation of the BYOD concept in business practices, mobile technology itself contributes to additional and more complex challenges. Enterprises are not the owners of those smart devices with access to enterprise networks and their data. *Fig.2* illustrates how smartphones with applications developed by unknown sources could be a threat to enterprise's sensitive data.

Business Drivers for Change

As introduced above an active need is emerging for more effective mobile solutions. It is not only a reflection of the compliance requirements but a real protective solution against mobile threats without any restrictions on financial growth or cutbacks on efficiency initiatives. There are compelling reasons to act and change now including data potentially at risk, pressure from regulatory bodies and audit firms to be compliant with the applicable data handling regulations, and the implementation of mobile security into an existing security structure.

Highlights of a Political-Economic-Social-Technology (PEST) Analysis

Politicians are setting high standards for data management regardless of platforms, even if they are related to mobile devices or mobile applications. These regulations mostly focus on the handling of financial data such as The Sarbanes–Oxley Act of 2002 (SOX). There are new developments regarding data (pictures, text, etc.) ownership such as The Stop Online Privacy Act (SOPA). The Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act or in short PROTECT IP Act (PIPA) will have an even more rigorous norm for enterprises who need to meet these regulations in order to obtain permission to operate in a certain field or market (market player).

The economic situation puts more pressure on businesses as the trend still shows stagnancy on a macro level while in some segments it is still in decline. Firms have high demands for business achievements measured by revenue and profit perspectives to meet shareholder expectations. One way to do so is to improve cost structures with mobile enablement (particularly BYOD).

Society wants to live more comfortably by searching for easily accessible services, such as online mobile-enabled bank transfers or online mobile retail orders. Companies aim to reach their customers via mobile applications that are more easily accessible through user-friendly interfaces, such as social network platforms. As usual, this trend is typical for major market areas, such as North America or, Western Europe; however, other regions are expected to follow.

The trend in technology continues to be more vivid from a computing power and portability perspective. Internet Service Providers are granting access to higher bandwidth networks for new applications and online content.

Policy Enforcement and its Weaknesses

To manage the various types of mobile devices in an enterprise, a solution was introduced in 2008 by STRICKLEN, MCHALE, CAMINETSKY and REDDY based on Pattern Definition for Mobile Device Management (MDM). MDM is the most common approach how mobile devices (including smartphones, tablets) are managed within the enterprise as a management tool for monitoring and policy enforcement. Even though this technology is available and wide-spread, according to ABI research, mobile threats grew by 261% just in the

last quarter of 2012; however, MDM technology is not growing at a comparable rate to the number of vulnerabilities and attacks.

One of the components of MDM is the registration module, which is responsible for identifying mobile devices within the enterprise network, where the identifier indicates the platform of each mobile device, e.g. smartphone and tablet. The other significant element is the management module. Its job is to receive a management function definition performed on mobile devices using identifiers from mobile devices. The management module is responsible for instructions for the first platform to perform the management tasks and provides instructions for the other modules specific to the second platform to perform the management task on at least the second device.

However, MDM is not the ultimate solution for mobile device security within the enterprise environment due to some concerns regarding the verifiable device integrity. There are attempts at identifying MDM solutions to detect modifications of the underlying platform, but since the MDM agent has limited privileges and was susceptible to compromise by malicious privileged software, these stand little chance of detecting a targeted attack. The US National Security Agency (NSA) describes an immutable cryptography, as the 'root of trust' on a specific platform, to be available for leveraging by MDM or other software, providing a means of countering this type of threats. Encryption enables devices to attest their integrity on an enterprise and carry out any local policy decisions. The availability of this 'root of trust' to other software can vigorously complement a chain of trust that begins when booting and extends into the system runtime. An additional benefit of an immutable root of trust is that it allows a company to bind the unique identifier of that device together with other credentials to restrict company access to only those devices. In effect, the device itself can become one of the factors of a multi-factor access.

In summary, MDM's current capabilities support the BYOD and enterprise-owned use of mobile devices with certain gaps for high-security issues. Management capabilities are limited to those provided for MDM products by the underlying mobile OS (iOS, Android, and other platforms), and therefore, these capability gaps cannot be closed by MDM providers alone. On-going cooperation between enterprise customers, OS vendors, and MDM vendors is critical to the continued advancement of enterprise-level security for mobile devices. Closing stated holes will enable the deployment of commercially available mobile devices to tackle high-security use issues common in sensitive industrial and governmental environments.

Secure data networks need to guarantee integrity, confidentiality and availability; this is when security is fulfilled. Policy enforcement with the MDM can be too liberal, but then there is no real need for MDM or strictly constraining users thus limiting the value-add. The proposed solution is to identify the user based on behaviour and compare behaviour changes.

Behaviour Analysis and Challenges

Growing recognition drove the importance of network science related to the behaviour of sophisticated systems that is shaped by relations among their constituent elements. The rising availability and tractability of large and high quality data sets on a wide range of complex systems [1-3] have led to a primary insight: substantially diverse complex systems often share core key organizational principles. These can be quantitatively characterized by the same parameters, which means that they show remarkably similar macroscopic behaviour despite reflective differences in the low-level details of the components of each system or their mechanisms of interaction.

The behaviour as described above can be modelled by mathematical graphs, where the graphs are defined simply as a set of nodes called vertices linked together in direct or indirect ways by connections (edges). From a mathematical point of view, $G(V, E)$ are canonical graphs as the vertices and edges are labelled. In network science, methodological advances permit research to quantify other topological properties of complex systems, such as modularity [4], hierarchy [5], centrality [6] and the distribution of network hubs [7,8]. There have also been significant efforts to form the development or evolution of complex networks [9], to link network topology to network dynamics, and to explore network robustness and vulnerability. These topics are likely to become more relevant in relation to behavioural studies.

Structural and functional behaviour maps can be created using graph theory through the following four steps:

1. Define the network nodes.
2. Estimate a continuous measure of association between nodes.
3. Generate an association model by compiling all pairs of associations between nodes and usually apply a threshold to each element of this model to produce a binary adjacency matrix or undirected graph.
4. Calculate the network parameters of interest in this graphical model of the behaviour network and evaluate them against the equivalent parameters of a population of random networks.

The elements such as defined network nodes, relationship of nodes, generated association matrix and network parameters give the basis of the behaviour type of "blueprint" of a user. A mobile user can be defined as an identity based on certain features of this behavioural "blueprint" as the key points of a fingerprint within the enterprise company. In *Fig.3* the darker highlighted edges could be the essential elements for the identifier.

Access to resource driven networks is defined in the graph theory as a set of nodes or vertices and the edges or lines, plus the connections between them. The graph topology can be quantitatively captured by a wide variety of measures used to generate the key points of the blueprint. The most important measurement is the node degree. The degree of a node is the number of

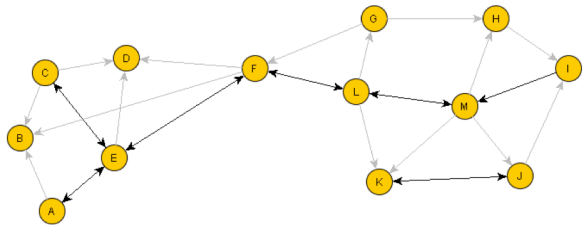

Figure 3: An example of a mobile user's identity on the basis of a "blueprint" network

connections it links to the rest of the network. Based on this definition, it is the most elementary network measure, and most other measures are ultimately linked to the node degree. The degrees of all the network's nodes identified form a degree distribution [10]. In randomly selected networks all of the connections are equally probable, i.e. the result is a Gaussian distribution. However, complex networks in general have non-Gaussian distributions, often with a long tail towards higher degrees. The degree distributions of the scale-free networks follow a power law [11]. This landmark study [11] was the first to describe the scale-free organization of many complex networks and proposed a simple growth rule for their formation.

The number of connections could give a large graph network that could be used for usability needs to define clustering, coefficients, and motifs. If the nearest neighbours of a node are also directly linked to each other, they form a cluster, and the clustering coefficient quantifies the number of connections that subsist between the nearest neighbours of a node as a quantity of the maximum number of possible connections [12]. The randomly selected networks exhibit low average clustering, whereas compound networks displays high clustering. Interactions between neighbouring nodes can also be counted by counting the occurrence of small motifs of interconnected nodes [13]. The distribution of different motif classes (nodes EFL and KMJ in *Fig.3*) in a network provides information about the types of local interactions that the network can support [14].

The numbers of reachable nodes and hops needed for connectivity are defined by the path length and efficiency. The path length is the minimum number of edges that must be passed through to start moving from one node to another. Random, complex networks have short mean path lengths; they exhibit high global efficiency of parallel information transfer, whereas regular patterns exhibit long mean path lengths. Efficiency is inversely related to path length. Nevertheless it is numerically easier to estimate topological distances between elements of disconnected graphs. Moreover, the link density or cost of the route provides further description. The connection density is the actual number of the network edges in the graph as a proportion of the total number of possible edges and is the simplest estimator of the physical cost of the network.

Hubs are nodes of high degree, where the centrality of a node measures how many of the shortest paths exist between all other node pairs in the network passing through it. It can be asserted that nodes with high centrality are thus crucial to efficient communication [15]. The importance of an individual node to network effectiveness can be assessed by deleting it and estimating the efficiency of the severed network. The robustness property refers either to the structural integrity of the network following the deletion of nodes, edges or effects of perturbations on local or global network states.

Finally, modularity is the property that has significant influence on the "blueprint" of the behaviour. There are algorithms that estimate the modularity of the network on the basis of hierarchical clustering [16]. Each module contains several densely interconnected nodes, and there are relatively few connections between these nodes in different modules. Airline hubs described this as a function of their roles in community structure [17]. Provincial hubs are connected mainly to nodes in their modules where the connector hubs are connected to nodes in other modules.

Graph Based Analysis of Smartphone Usage

Previously, the challenges of using mobile devices in the enterprise environment were discussed. It is important to identify the activities on the device in order to take either preventive or corrective actions. $G(V, E)$ used for the behaviour identification and description graphs. Vertices are defined as applications, more precisely, vertices within the device or network addresses and sites. Edges are the connections between the vertices applications called websites, network addresses, user- or process-initiated connections.

- Network nodes can be defined as the resource access, i.e. applications, programs, and device elements access initiated by the user or application calls.
- Association between network nodes could be defined as the connections of the applications (calls, connections, as web access), usually resources are connecting together.
- Based on the above elements, network nodes and associations provide the details to calculate the association matrix.
- The following steps include network parameter analysis calculated from the above.

The question is not whether mobile activity can be defined as a complex network and describable by graph, but whether the process identies a user by a motif. However, before this question can be answered certain challenges need to be faced:

- identify motifs as maximum independent set,
- search motif in the complex network,
- define „approved behaviours" according to the identification of user behaviour.

Identification of the Motif in the Graph

The task is to find the Maximum Independent Set (MIS) of a particular graph as was defined by GAREY and JOHNSON [18] as NP-complete and remains so even for bounded degree graphs. According to FEIGE *et al*. [19] MIS cannot be approximated even within a factor of $|V|^{1-o(1)}$ in polynomial time.

The greedy algorithm (GMIS) can provide a solution for the identification of the maximum independence set. The algorithm selects a vertex of minimum degree, deletes that vertex and all of its neighbours from the graph, and repeats this process until the graph becomes empty. A recent detailed analysis of the GMIS algorithm has shown that it produces reasonably good approximations of the MIS for bounded- and low-degree graphs defined by HALLDORSSON and RADHAKRISHNAN [20]. In particular, for a graph G with a maximum degree Δ and an average degree $\bar{d}$, the size $|I|$ of the MIS satisfies *Eq.(1)*.

$$|I| \leq \min\left(\frac{\Delta+2}{3}|\mathrm{GMIS}(G)|, \frac{\bar{d}+2}{2}|\mathrm{GMIS}(G)|\right) \quad (1)$$

where |GMIS(G)| is the size of the approximate MIS found by the GMIS algorithm.

Eq.(1) provides an upper-bound of the number of edge-disjoint embeddings of a particular sub-graph, and will use this bound to obtain a computationally tractable problem formulation that is guaranteed not to miss any sub-graphs that can potentially be frequent.

Searching for a Discover Motif in the Graph

The GROCHOW-KELLIS method [21] can be used to find all examples of sub-graphs of a given size, similar to exhaustive methods. In the background, all non-isomorphic graphs are generated of a particular size using MCKAY'S tools [22]. Then for each graph, the method evaluates its significance. Due to symmetries, a set sub-graph of G may be mapped to a set query graph H multiple times. Therefore, a simple mapping-based search for a query graph will locate every case of the query graph as many times as the graph has symmetries. To avoid this, the method computes and enforces several symmetry-breaking conditions, which ensure that there is an exclusive map from the query graph H for each case of H in G, so that the search only spends time finding each instance once

```
IsomorphicExtensions (f,H,G[,C(h)]:
Finds all isomorphic extensions of partial map f :
   H → G [satisfying C(h)]
Start with an empty list of isomorphism.
Let D be the domain of f.
If D=H, return a list consisting solely of f.
   (Or write to disk.)
Let m be the most constrained neighbour of any d ∈ D
   (constrained by degree, neighbours mapped)
For each neighbour n of f (D)
If there is a neighbour d ∈ D of m such that n is not
   neighbours with f(d),
or if there is a non-neighbour d ∈ D of m such that n
   is neighbours with f(d)
[or if assigning f (m)=n would violate a symmetry-
   breaking condition in C (h)],
then continue with the next n.
Otherwise, let f=f on D, and f (m)=n.
Find all isomorphic extensions of f.
Append these maps to the list of isomorphism.
Return the list of isomorphism
```

The symmetries of a graph H equals automorphism (self-isomorphism). The collection of automorphism of H is indicated by $Aut(H)$. For a set A of automorphism, two nodes are stated to be "A-equivalent" if there is some automorphism in A which maps one to the other, or just "equivalent" if A $=Aut(H)$. Given a set of conditions C, α preserves the conditions C if, given a labelling L1 of H which satisfies C, the corresponding labelling L2: $H \rightarrow Z$ given by $L2(n) = L1(\alpha(n))$ also satisfies C. We are thus searching for setting C, such that the only automorphism preserving C is the identity. This ensures exactly one map from H onto each of its instances in G to satisfy the conditions. To find these conditions, an $Aut(H)$-equivalence class $\{n_0, ..., n_k\}$ of nodes of H, and the condition $L(n_0) < \min(L(n_1), ..., L(n_k))$ imposed. Any automorphism must send n_0 to one of the n_i, since these are all of the nodes equivalent to n_0. However to preserve this state, an automorphism must send n_0 to itself. Then the process continues recursively, replacing $Aut(H)$ with set A of automorphisms that send n_0 to itself. Because `FindSubgraphInstances` starts with a particular node that node can be considered already fixed.

The main reasons for the selection of the GROCHOW and KELLIS method are summarized as follows:

- Capable of finding more significant motifs by enabling exhaustive discovery of motifs up to seven nodes. To find even larger motifs, the method samples a connected subgraph, and then finds all its occurrences and assesses their significance using this method. This practice has enabled the algorithm to find motifs of up to fifteen nodes and examine subgraphs of up to thirty-one nodes;
- Capable of quering a particular subgraph by querying whether a particular subgraph is significant;
- Capable exploring motif clustering; because the algorithm finds all occurrences of a given subgraph, it can be used to examine how these cases cluster together to form larger structures;
- Time and space applied to all subgraphs of a set size, takes exponentially a smaller amount of time than previous methods, even when implementing the previous method with the hashing scheme.

Conclusions

Apparently the current policy enforcement solutions are not sufficient because they mainly focus on policy compliance based on the response of the device. The installation of malicious applications could alter the mobile devices response (jailbreak on IOS or Android

and software imitating a response to the MDM server) taking to more serious security issues. Similarly to the recently identified malware `Oldboot.B`, which can install malicious applications in the background, it can inject malicious modules into the system process that prevents malware applications from uninstalling. `Oldboot.B` can change the browser setup (set a new and unwanted home page), and it also can uninstall or disable installed Mobile Antivirus software, and even steal data such as credit card information or any other critical data. This malware is especially dangerous as it implements evasion techniques to stay undetected. In order to optimize current threat detection, which is also in line with business requirements, additional and different methodologies are required such as user identification based on the blueprint of the behaviour of the user.

To create a working model of the graph-based user identification, several tasks await completion. The running tasks are the edges started by the system or user defined as the connections between them. Once the complex network and graph are set up the motif can be identified with a greedy algorithm and search of the global graph with the GROCHOW-KELLIS Algorithm. In order to have a behaviour-based decision making system, all of the above algorithms will be tested to further develop the behaviour-based system.

REFERENCES

[1] AMARAL L.A.N., SCALA A., BARTHELEMY M., STANLEY H.E.: Classes of small-world networks, Proc. Natl Acad. Sci. USA *2000*, 97, 11149–11152

[2] AMARAL L.A.N., OTTINO J.M.: Complex networks. Augmenting the framework for the study of complex systems, Eur. Phys. J. B *2004*, 38, 147–162

[3] BARABÁSI A.L., OLTVAI Z.N.: Network biology: understanding the cell's functional organization, Nature Rev. Genet. *2004*, 5, 101–113

[4] GIRVAN M., NEWMAN M.E.J.: Community structure in social and biological networks. Proc. Natl Acad. Sci. USA *2002*, 99, 7821–7826

[5] RAVASZ E., BARABÁSI A.L.: Hierarchical organization in complex networks, Phys. Rev. E Stat. Nonlin. Soft Matter Phys. *2003*, 67, 026112

[6] BARTHÉLEMY M.: Betweenness centrality in large complex networks, Eur. Phys. J. B *2004*, 38, 163–168

[7] GUIMERA R., AMARAL L.A.N.: Functional cartography of complex metabolic networks, Nature *2005*, 433, 895–900

[8] GUIMERA R., MOSSA S., TURTSCHI A., AMARAL L.A.: The worldwide air transportation network: anomalous centrality, community structure and cities' global roles, Proc. Natl Acad. Sci. USA *2005*, 102, 7794–7799

[9] KASHTAN N., ALON U.: Spontaneous evolution of modularity and network motifs, Proc. Natl Acad. Sci. USA *2005*, 102, 13773–13778

[10] AMARAL L.A.N., SCALA A., BARTHELEMY M., STANLEY H.E.: Classes of small-world networks, Proc. Natl Acad. Sci. USA *2000*, 97, 11149–11152

[11] BARABÁSI A.L., ALBERT R.: Emergence of scaling in random networks, Science *1999*, 286, 509–512

[12] WATTS D.J., STROGATZ S.H.: Collective dynamics of "small-world" networks, Nature *1998*, 393, 440–442

[13] AMARAL L.A.N., OTTINO J.M.: Complex networks. Augmenting the framework for the study of complex systems, Eur. Phys. J. B *2004*, 38, 147–162

[14] BARABÁSI A.L., OLTVAI Z.N.: Network biology: understanding the cell's functional organization. Nature Rev. Genet. *2004*, 5, 101–113

[15] FREEMAN L.C.: A set of measures of centrality based on betweenness, Sociometry *1977*, 40, 35–41

[16] GIRVAN M., NEWMAN M.E.J.: Community structure in social and biological networks. Proc. Natl Acad. Sci. USA *2002*, 99, 7821–7826

[17] GUIMERÀ R., MOSSA S., TURTSCHI A., AMARAL L.A.: The worldwide air transportation network: anomalous centrality, community structure and cities' global roles. Proc. Natl Acad. Sci. USA *2005*, 102, 7794–7799

[18] GAREY M.R., JOHNSON D.S.: Computers and Intractability: A Guide to the Theory of np-completeness. New York: W. H. Freeman and Company, *1979*

[19] FEIGE U., GOLDWASSER S., LOVASZ L., SAFRA S., SZEGEDY M.: Approximating clique is almost NP complete, Proc. 32nd IEEE Symposium on Foundations of Computer Science (FOCS), *1991*, 2–12

[20] HALLDORSSON M.M., RADHAKRISHNAN J.: Greed is good: Approximating independent sets in sparse and bounded-degree graphs, Algorithmica, *1997*, 18(1), 145–163

[21] GROCHOW J.A., KELLIS M.: Network Motif Discovery using Subgraph Enumeration and Symmetry-Breaking, Computer Science and AI Laboratory, M.I.T. Broad Institute of M.I.T. and Harvard, *2007*

[22] MCKAY B.D.: Isomorph-free exhaustive generation, J. Algorithms, *1998*, 26, 306–324