MOBILE DEVICES AND EFFECTIVE INFORMATION SECURITY

Blaž Markelj[1], Igor Bernik[2]

Abstract

Rapidly increasing numbers of sophisticated mobile devices (smart phones, tab computers, etc.) all over the world mean that ensuring information security will only become a more pronounced problem for individuals and organizations. It's important to effectively protect data stored on or accessed by mobile devices, and also during transmission of data between devices and between device and information system. Technological and other trends show, that the cyber threats are also rapidly developing and spreading. It's crucial to educate users about safe usage and to increase their awareness of security issues. Ideally, users should keep-up with technological trends and be well equipped with knowledge otherwise mobile technology will significantly increase security risks. Most important is that we start educating youth so that our next generations of employees will be part of a culture of data and information security awareness.

Keywords: information security, blended threats, mobile devices, awareness.

Introduction

Mobile devices are constantly being developed and technologically improved so as to better facilitate access to data which is vital in decision-making and has become indispensable both in business and private life. Constantly available and unhindered access to data is no longer a luxury but a necessity. The evolution of the Internet, mobile devices, cloud computing, and relevant software, is focused on maintaining stable connections to corporate data, no matter where decision-makers are based and when they need to tap into their databases. A study conducted by comScore (Internet 1) showed that in November 2011 the Internet was used by 380 million Europeans.

[1] Blaž Markelj is an assistant at the Faculty of Criminal Justice and Security (blaz.markelj (at) fvv.uni-mb.si).
[2] Ph.D. Igor Bernik is an Assistent Professor at the Faculty of Criminal Justice and Security and Vice Dean for Academic Affairs (igor.bernik (at) fvv.uni-mb.si).

Experts at MicrostoftTag (Internet 4) estimate that by 2014 the number of mobile connections to the Internet will surpass the number of connections made by stationary computer equipment; the current ratio is 50:50. Only uninterrupted connections to the Internet guarantee constant/unlimited access to data, and mobile devices are the connective elements between users and information system or data storages.

But constant access to data also has its downsides. Users of mobile devices can easily become targets of numerous threats, such as malicious code, viruses, intercepted communications, theft of data or mobile device, mobile device thefts, etc. Numerous global manufacturers and providers of security software report that virus infections are increasingly spreading, there are more reports of unauthorized GPS location tracking of mobile device users, misappropriations of personal and confidential data (certificates, passwords, etc.), and automatic "plantings" of bits of malicious code. These are only a few examples of the possible forms of attacks on mobile devices, which are indeed forms of cyber-crimes. Cyberspace provides numerous beneficial opportunities, but it also poses certain dangers (Bernik, Prislan, 2012). Regrettably users' awareness of cyber-crime is mostly derived from and influenced by mass media (Bernik, Meško, 2011: 242 - 252).

Cyber attacks can be deterred only if users adhere to certain procedures (and are familiar with certain functions of their hardware and software) and conduct themselves in such a manner as to protect data from being alienated when attacks are detected. Corporations should educate their employees and inform them about security measures and the basics of protecting digital evidence, in case they experience cyber threats or attacks. Proper evidence protection is important because it increases the likelihood that perpetrators will be caught.

The information infrastructure within which data is stored should be designed so as to be compatible with the functions of mobile devices, but data should also be sufficiently protected. In the past, remote access was provided by an »open door« in the system's fire wall through which communication could flow. Sophisticated mobile devices now constantly maintain connections with the Internet, and so communication mostly flows in a general way, as intended for web communications (browsing). This means that a door in the firewall is constantly left open and unprotected, thus increasing the possibility the system will be violated.

In addition to storing and processing data in their own information systems, more and more organizations are now entrusting their data to

clouds. Because cloud technology works on an automated virtual plane the distribution of a system's resources is an automatic function of the system. It's necessary to provide sufficient protection from threats and see that digital evidence is properly collected in the event of a security incidence, so that the perpetrator can be detected and prosecuted. Detection is often difficult because a perpetrator's location is remote, and usually unknown. Users should careful choose their cloud provider. Since increasing numbers of corporations are now using cloud computing, the risk of experiencing threats is growing. TechNavio published a report on the current spread of cloud computing and the estimated future growth of these services – a 42 % growth rate is expected between 2010 and 2014 (Internet 5).

Mobile Devices as Security Risks

The weakest link in the whole "mobile system", especially the process of storing and transferring data, is the user, be it an individual or corporation or other type of organization. In general, users are more or less educated about mobile devices, cloud computing, software, data transference, and the safe use of this technology. Our findings show that users aren't keeping-up with technological developments and are therefore relatively unprotected from the continuously evolving cyber threats. Statistical data from the past few years confirms that the number of infected mobile devices is growing. Both Lookout (Internet 3) and Juniper (Internet 2) regularly report more and more incidences of malware infections.

The question is why anyone would still want to penetrate a corporate information system or cloud directly since it's possible to get all the desired data through mobile devices which are now so often used to access corporate systems via different networks, and are more often than not, inefficiently protected. The IDC study (Internet 7) showed that, globally, sales of mobile smartphones are going up by 50 % per year. According to the CEE Telco Industry Report, carried out by GfKGroup (Internet 6) in 15 Central and Eastern European states, Slovenia is leading with the most smartphone users (27.8 % of Slovenians use smartphones). The second in line is Turkey (23.7 % use smartphones), followed by Lithuania (18.5 %). The more there are users of mobile technologies the greater the exposedness of information systems to security risks. Threats are becoming more sophisticated and cybercrime is on the rise, because more mobile devices in use present more opportunities for perpetrators.

As we know, data which can be accessed by using mobile devices and Internet connections can be stored at different locations, that's why

threats have to be categorized and each type tackled differently. Threats arise individually or in combinations (Markelj, Bernik, 2011), but the perpetrators' intention is always to illegally get hold of confidential data and information that have a monetary value. It is vital to identify: locations/points where threats could present themselves, types of threats, and the possible damaging consequences of realized threats.

Corporate information systems and cloud computing can be especially vulnerable, even though indirectly, because employees now almost all frequently use mobile devices and have (open) accesses to sensitive data. Especially vulnerable are organizations which don't use even the most basic protection (e.g., authentication, encryption, tunnel protocols, secure Internet connections, etc.).

Beckham (2011) drew attention to five major information security risks related to cloud computing and compounded by mobile device usage. First there is the transfer of data between a corporate information system, a mobile device and cloud. Especially risky is transferring data by using various different Internet providers and simultaneously not encrypting data or using authentication and secure Internet connections (http, etc.). The second problem is the software interface, and the way in which users are verified when they access data in a cloud. Other dilemmas of information security are related to how data is stored, how it is diffused, and whether it's encrypted. Is data encrypted all the time, even while it's being transferred to a device and/or stored on a server? The need to maintain constantly available accesses to data – and therefore being dependant on Internet connections – is quite a big security risk.

Currently Available Security Solutions

Security threats come in many forms and they are rapidly evolving. Many corporations now have mobility at the center of their IT strategy, and it would serve them well to put new emphasis on their strategy for maintaining the information security of mobile device (Mathias, 2011). Milligan (2007: 189–193) noted in his article that corporations and other organization can't monitor something that can't be identified. What the author had in mind, were threats endangering corporations represented by the usage of the rapidly evolving mobile devices and information technology in general. Therefore, corporations should constantly upgrade their information security policies and assess the cyber threat risk levels.

Corporations often minimize risk by implementing hardware that detects potential dangers at the level of Internet traffic (Whitman, Mattord, 2008),

and special equipment that prevents information system break-ins (Scarfone, Mell, 2011). Some companies that are developing security software are already providing advanced software solutions for mobile devices (Schechtman, 2011) and firewalls which monitor Internet traffic on the mobile device and the information system (Endait, 2010). Specific software solutions enable corporations to define their own safety guidelines for the usage of mobile devices (Mottishaw, 2010). Employees usually have passwords to wireless networks (Arbaugh, 2003).

Corporations can protect their data by using encryption software, but this method of protection is only as strong as the encryption key itself. It is possible to encrypt only certain segments of data stored on a mobile device, or data transferred through the Internet, or an information system as a whole. The encryption should in no way hinder the functions of a mobile device. Gilaberte (2004: 299-304) wrote about various methods and algorithms, which can be used to encrypt certain data in certain ways.

Corporations also strive to achieve better information security, especially in regard to log-on procedures, and/or the transfer of crucial data and information. This can be accomplished by implementing safer »http« data transfer protocols, and by authentication with certificates, as well as by encrypting and decrypting data (SSL), and also by the use of virtual private networks (VPN). Good examples of how the above-mentioned technology is used are bank portals and portals used for managing email. Certificates are used to authenticate the identity of a user when he or she tries to access these portals. Corporations try to protect their data by using strong passwords and authentication by a smart-card. Smart-cards can function only, if supported by sophisticated »background« technology.

Most organizations set up virtual private networks to enable direct communication between mobile devices and their corporate information system or systems. This technology functions on the principle of establishing a channel between the virtual private network software of the mobile device and the virtual private network server located within a corporation's information system. Verification between a mobile device and an information system is done by using certificates – entrance to the system is granted once the identity of the user is verified (username, password).

Zheng Yan and Peng Zhang (2006: 1057–1064) noted that we should be aware of two crucial security weaknesses in the virtual private network

technology. These are: (1) software for mobile devices and virtual private network clients are so diverse that it's impossible to guarantee that the technology will work flawlessly; (2) it's questionable, whether the software on a mobile device (including specific software used to establish a connection to a virtual private network) can be fully trusted. As noted by Milligan (2007: 189-193) some security measures in use today can't efficient protect mobile devices against blended threats.

Research Method and Result

Understanding how smartphones are actually used is of crucial importance to the future technological development and implementation of information security. It's undeniable that for students mobile devices have become indispensable communication tools, so it's even more important that we find out which elements of information security these users are familiar with, and use them, because this generation will soon be working in corporate environments and routinely using different mobile devices.

These issues were the basis for our online study conducted in December 2012. Our questionnaire was published on the web portal »1ka« (www.1ka.si) for 21 days. We alerted youth to our survey through e-mail, Facebook profiles, and in person. The questionnaire was designed so that we would discover how and why students used their mobile devices; specifically which devices and software solutions they preferred. The second part of the questionnaire was designed so that we could gauge users' knowledge and use of security measures, and determine their awareness of cyber threats endangering data security. The analysis of the compiled survey data was made with SSPS software tools.

Because some questionnaires weren't filled out completely, the sample population for some questions varies. Most of the respondents were aged between 21 and 25 years, in the next group were youth under 20 years of age. 61.5 % of the respondents were female, 63.2 % were male; all had secondary school level education. Table 2 shows what the respondents used their mobile devices for (in this case smartphones). More than a half of the respondents used smartphones for personal purposes, while a quarter of them use them for both personal and work related purposes. Because of the chosen sample population, these finding were more or less expected (Table 1). It gives us concern that the percentage of users who used the same mobile device for private affairs and business purposes is relatively high.

Table 1: Characteristics of the sample population – users of the World Wide Web

		N	%
Age (n=281)	below 20 years	75	26.7
	21 to 25 years	133	47.3
	26 to 34 years	57	20.3
	35 to 44 years	2	4.6
	44 to 54 years	2	0.7
	Over 55 years	1	0.4
Gender (n=275)	female	169	61.5
	male	106	38.5
Education level (n=280)	secondary school	177	63.2
	1st Bologna level	67	23.9
	2nd Bologna level	25	8.9
	3rd Bologna level	11	3.9

Source: Blaž Markelj, Igor Bernik

Table 2: Smartphones are used for

Sample (n=216)	N	%
only for personal needs	126	58.3
for personal needs, occasionally also for business needs	56	25.9
for personal and business needs	31	14.4
for business needs, occasionally also for personal needs	1	0.5
only for business needs	2	0.9

Source: Blaž Markelj, Igor Bernik

The question is whether students' habits are already such that they have difficulty drawing a line between private and business affairs. How will

youth use mobile technologies in the near future? Is it possible to change the present trend and ensure better security of data and information? It's problematic when private and corporate data is indiscriminately mixed without ensuring sufficient security. The results derived from a study conducted by Ponemon (2011) also showed a high percentage (40 %) of people who used mobile smartphones for private and business needs. We can conclude, based on the finding of Ponemon's and our own survey, that, in the future, it will be increasingly difficult to delineate between private and business usage of continuously improving mobile devices.

The Security Dilemmas of Mobile Devices

The analysis of the data compiled in the course of our study showed us how the student population uses mobile devices and what kinds of connections to cyberspace they use. Our aim was to determine how well young users are aware of certain cyber threats and the various protective measures which they could use to avoid loss of data and other security incidences. We found out that the most commonly known cyber threats were theft (89.4 %) and viruses (83.1 %) followed by bluetooth hacking, tracking, payment frauds, infections through applications, data alienation, interception of communications, automatic data transfer, browser infection, spyware infection, drive-by-downloads, malware infection, phishing, and rootkit infection. These findings aren't surprising, because all the above mentioned threats have been around for some time and are relatively well known. What gives us cause for concern is that youth aren’t better informed about the sophisticated malware that is steadily proliferating and spreading. Corporations and larger organizations regularly publish periodical security reports and analyses, which consistently show a steady rise in the number of mobile devices infected by malware. The results of our study show that users aren’t well aware of these threats and are unprepared to deal with them.

Table 3 shows some possible and available solutions which can effectively protect mobile devices from cyber threats. Most participants in our study answered that they do use standard PIN-code protection for their SIM-cards and antivirus software, but said that they aren't aware of the more sophisticated tools, such as data encryption and remote deletion of data from mobile device, and didn’t use them.

Table 3: Protective measures for mobile smartphones

	I use	I'm familiar with, but I don't use	I'm not familiar with
PIN-code for SIM-card	89.6%	9.9%	0.5%
antivirus protection	29.5%	49.3%	21.3%
education	26.0%	41.2%	32.8%
PIN-code for applications	21.4%	56.8%	21.8%
smartphone tracking	20.3%	50.2%	29.5%
contents archiving	19.5%	44.4%	36.1%
authentication	13.0%	43.3%	43.8%
remote content deletion	6.8%	40.8%	52.4%
VPN connection	6.8%	40.8%	52.4%
central control	6.3%	40.5%	53.2%
data encryption	5.8%	54.4%	39.8%

Source: Blaž Markelj, Igor Bernik

A small number of respondents (9.9 %) confirmed that they are aware of certain other protective measures, such as PIN-codes, but don't use them. Looking at the results of our survey, it's safe to say that young users aren't sufficiently aware of and informed about all the different threats to information security, especially the most sophisticated ones, and don't know enough about protective measures, therefore it's hard to prevent certain security incidences, misusages of mobile devices and data theft, even though some good technical solutions are available.

As we said many corporations periodically publish the results of their surveys which all show that the number of smartphones infected with malware is steadily growing, on the other hand our study showed that the student population is relatively uninformed and unprepared to meet these challenges to information security. It's a fact that the youth of today will soon join the ranks of employees in corporations and other organizations where they will access and manipulate confidential corporate data by using various mobile devices.

Conclusion

Mobile devices come with some protective measures preinstalled, but users often ignore them. Information security depends on how much individuals know about the technology they use, therefore it's crucial to

spread awareness and implement organizational policies to regulate the use of mobile devices, software, and accesses to corporate data in central information systems and/or cloud. It's necessary to evaluate which data can be stored on mobile devices, which in the information system and cloud, and of course, whether it's safe to access data from remote locations.

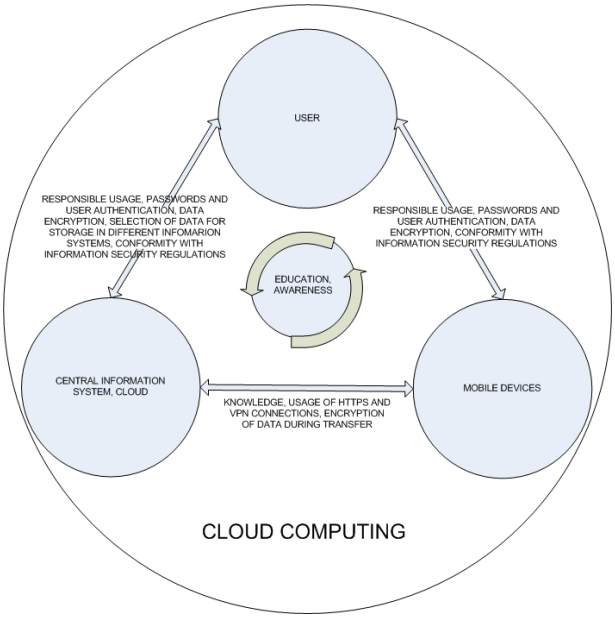
Figure 1 shows some security measures that can be implemented to protect connections between mobile devices and central information systems and/or cloud, but the human factor is still the most crucial. It all comes down to the question, how much users of mobile devices know about information and communication technology and how well aware they are of the potential dangers. The outline in Figure 1 is based on theory and the findings of our study. The conclusions are focused on drawing attention to the rising trend in the number of threats endangering users of mobile devices and all who access corporate data from remote locations. All mobile devices users should be informed which threats they could encounter, what the consequences could be, and, of course, be told how to avoid them.

On one hand, there are different methods of protecting oneself against cyber threats, but one has to use them. On the other hand, there are also many ways to alienate data. The most common are: theft of mobile device, interception of data, and direct breach of an information system. Systems can also be broken-into by using decoding methods or by stealing passwords. But there are even more sophisticated ways which can »open a system's back door« or retrieve data by infecting the system with malware. Infected mobile devices can automatically pass on confidential information (certificates, passwords, the location of the user, etc.) to unauthorized strangers.

Mark Fischetti (2011) made a list of the most commonly used methods of data alienation. At the top of his list are violations of corporate computers and server systems (16 %). We can immediately draw parallels with the results gained through studies carried out by Lookout (Internet 3) and Juniper (Internet 2), which indicate a significant increase of different infections; and our study from 2011 of how well Slovenian users of mobile devices are aware of the threats and available protection. Obviously, all three studies show that the quantity of malware is increasing which increases the likelihood that more systems will get penetrated more frequently. The second most common method of data alienation is the direct »harvesting« of data off the web. This can also be compared to an infection since perpetrators can access a user's data on the web only if they know his password to his profile or data storage in a

cloud. It's interesting that in our study theft and viruses were at the bottom of the list of the data alienation methods most commonly known by young users.

Figure 1: Security measures for connections between mobile devices and a central information systems and clouds.



Source: Blaž Markelj, Igor Bernik

Studies don't show a decrease in the proliferation of cyber threats to mobile devices, and consequently, a decrease in the number of misusages and data thefts – quite the contrary. Manufacturers of information security products are well aware of this fact. For the future, industry guidelines foresee further evolution of security software, especially of software that will be activated (by a password) whenever a user logs-on to an information system, and will be in compliance with a company's security policy. Trends in information security solutions point towards rising users' awareness of cyber threats, promoting knowledge about new technologies, and informing people about the available protective measures.

Resources

Arbaugh, William A. (2003): Wireless Security Is Different. IEEE Computer. Vol.: 36, No.: 8, pp.: 99-101.

Beckham, Jeff (2011): The Top 5 Security Risks of Cloud Computing. Available at: http://blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud-computing (30.12.2011)

Bernik, Igor, Prislan, Katja (2012): Cybercrime, Security Risk to Information System, Cyber Terrorism (Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem). Ljubljana: Fakulteta za varnostne vede.

Bernik, Igor, Meško, Gorazd (2011): Internet Analysis of Knowing Cyber Threats and Fear Against Cybercrime (Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto). Revija za kriminalistiko in kriminologijo. Vol.: 62, No.: 3, pp.: 242 – 252.

Endait, Sneha (2010): Mobile Security – The Time is Now. Available at: http://www.authorstream.com/Presentation/snehaendait-477029-mobile-security/ (5.3.2011)

Fischetti, Mark (2011): Stolen data: How thieves get your identity and other information. Scientific American. Available at: http://www.scientificamerican.com/article.cfm?id=data-breach-how-thieves-steal-your-identity-and-information (30.12.2012)

Internet1:http://www.comscore.com/Press_Events/Press_Releases/2012/1/Nearly_50_Percent_of_Internet_Users_in_Europe_Visit_Newspaper_Sites (2.2.2012)

Internet 2: http://www.juniper.net/us/en/dm/interop/go (10.9.2011)

Internet 3: https://www.mylookout.com/mobile-threat-report (10.9.2011)

Internet 4: http://www.digitalbuzzblog.com/2011-mobile-statistics-stats-facts-marketing-infographic/ (2.2.2012)

Internet 5: http://www.marketresearch.com/Infiniti-Research-Limited-v2680/Global-Cloud-Systems-Management-Software-6458283/view-stat (7.9.2011)

Internet 6: http://www.gfk.com/group/press_information/press_releases/008894/index.en.html (6.6.2011)

Internet 7: http://www.idc.com/getdoc.jsp?containerId=prUS22871611 (9.9.2011)

Lacuesta, Gilaberte, Raquel (2004): Encryption tools for devices with limited resources. 4th WSEAS International Conference on Applied Informatics and Communications. Conference Proceedings, WSEAS. No.: 5, pp.: 299 – 304.

Markelj, Blaž, Bernik, Igor (2011): Information Security Threats in the use of Mobile Devices. New Situations and opportunities in Information Technology as a Result of Social Changes (Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. Nove razmere

in priložnosti v informatiki kot posledica družbenih sprememb). 18. konferenca Dnevi slovenske informatike.

Mathias, Craig (2009): Mobile Security Threats. Available at: http://searchmobilecomputing.techtarget.com/tip/Mobile-security-threats (20.10.2011)

Mayer, Milligan, Patricia (2007): Business Riskand Security Assessement for Mobile Device. 8th WSEAS International Conference on Mathematics and Computers in Business and Economics. Conference Proceedings, WSEAS. Vol.: 8, pp.: 189-193.

Mottishaw, Peter (2010): Policy Management Will Be Critical to Mobile Operators as Data Traffic Grows. Available at: http://www.analysysmason.com/About-Us/News/Newsletter/Policy-management-has-become-an-urgent-issue-for-mobile-operators-as-a-result-of-the-rapid-growth-in-mobile-data-traffic-increasing-availability-of-flat-rate-data-plans-and-new-regulations-in-Europe (6.3.2011)

Scarfone, Karen, Mell, Peter (2007): Guide To Intrusion Detection and Prevention System. Available at: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf (4.3.2011)

Schechtman, Dave (2011): IPad Security from En Pointeand McAfee's Mobile Security Practice. Available at: http://www.enpointe.com/blog/ipad-security-en-pointe-and-mcafees-mobile-security-practice (5.3.2011)

Whitman, Michael E., Mattord, Herbert J. (2010): Management of Information and Security, 2nd edition, Boston: Course Technology.

Yan, Zheng, Zhang, Peng (2006): Enhancing Trust in Mobile Enterprise Networking. 5th WSEAS International Conference On Applied Computer Science. Conference Proceedings, WSEAS. pp.: 1057-1064.

Innovative Issues and Approaches in Social Sciences

IIASS is a double blind peer review academic journal published 3 times yearly (January, May, September) covering different social sciences: political science, sociology, economy, public administration, law, management, communication science, psychology and education.

IIASS has started as a SIdip – Slovenian Association for Innovative Political Science journal and is now being published by CEOs d.o.o. (Slovenia) in association with the Institute for Social Change Research at the School of Advanced Social Studies (SASS) and the Faculty for Media (FAM) Slovenia.

Editor in chief: Albin Panič

Typeset
This journal was typeset in 11 pt. Arial, Italic, Bold, and Bold Italic; the headlines were typeset in 14 pt. Arial, Bold

Abstracting and Indexing services
COBISS, International Political Science Abstracts, CSA Worldwide Political Science Abstracts, CSA Sociological Abstracts, PAIS International, DOAJ.

Publication Data:
CEOs d.o.o.

Innovative issues and approaches in social sciences, 2013, vol. 6, no. 2

ISSN 1855-0541

Additional information: www.iiass.com

Innovative Issues and Approaches in Social Sciences (IIASS)

Editorial correspondence
All correspondence or correspondence concerning any general questions, article submission or book reviews should be addressed to info@iiass.si.

Subscription to IIASS
IIASS is available free of any charge at http://www.iiass.com under . You can sign in for a free newsletter.

Advertising
Please find our advertising policy at http://www.iiass.com For additional questions or inquiries you can contact us on e-mail info@iiass.si.

Language
The objective of academic journal is to provide clear communication with an international audience. Style and elegance is secondary aim. In this manner we allow US and UK spelling as long as it is consistent within the article. Authors are responsible for language editing before submitting the article.

Notes for Contributors
Please refer to www.iiass.com for detailed instructions. Sample layout can be downloaded from http://www.iiass.com/uploaded_articles/IIASS_layout.doc

Scope:
IIASS is electronic peer reviewed international journal covering all social sciences (Political science, sociology, economy, public administration, law, management, communication science, etc.). Journal is open to theoretical and empirical articles of established scientist and researchers as well as of perspective young students. All articles have to pass blind peer review.

IIASS welcomes innovative ideas in researching established topics or articles that are trying to open new issues that are still searching for its scientific recognition.

Additional information is available on: www.iiass.com