Tomasz BILSKI[1]

Poznań University of Technology (1)

doi:10.15199/48.2016.12.59

New Challenges in Network Security

Abstract. *The purpose of the paper is to point out different security issues of network evolution and to point out new threats related to the network evolution. We will discuss such issues as: complexity of security tools, IPv4/IPv6 transition, new modes of operation, IoT (Internet of Things), BYOD (Bring Your Own Device), cloud computing, SDN (Software Defined Network), wireless transmission. The paper should be of interest to different groups of people, among them are researchers and designers in the security area, policy makers and users of modern networks.*

Streszczenie. *Celem jest wskazanie aspektów bezpieczeństwa związanych z ewolucją sieci komputerowych. Przedstawiono takie zagadnienia jak: złożoność narzędzi bezpieczeństwa, przejście z IPv4 na IPv6, nowe tryby działania, Internet Rzeczy, BYOD (Bring Your Own Device), przetwarzanie w chmurach, SDN (Software Defined Network), transmisja bezprzewodowa. Artykuł powinien zainteresować różne grupy, w tym: osoby badające i projektujące zabezpieczenia, twórców polityk bezpieczeństwa i użytkowników sieci. (**Nowe wyzwania dla bezpieczeństwa sieci komputerowych**).*

Keywords: computer networks, data security, IoT, SDN, cloud computing, wireless transmission.
Słowa kluczowe: sieci komputerowe, ochrona danych, IoT, SDN, przetwarzanie w chmurach.

Introduction

Computer networks continuously evolve. The evolution is qualitative as well as quantitative. The quantitative complexity of Internet is constantly growing – for example:

- number of Internet users passed 3 billion,
- number of different devices connected to the Internet is estimated at the level of 8-10 billion,
- the pool of common BGP (Border Gateway Protocol) routes has increased from ~355 000 entries in January 2011 to more than 523 000 entries at the end of 2014,
- five Regional Internet Registries exhausted their general use pools of IPv4 addresses [9].

Qualitative modifications are visible in many different areas: communication protocols, hardware, software, approaches to network management, system/network virtualization, network applications, legal regulations for data transfer, user behaviour and awareness, cost of hardware reduction. Some of the key changes are: IPv4-IPv6 transition and dual-stack architecture, SDN, NFV (Network Functions Virtualization), IoT, BYOD, BYOW (Bring Your Own Wearable Devices), cloud computing, data storage virtualization, communication systems convergence, big data services, much greater number of interconnections between systems. Incorporating IP protocol in mobile phone networks (in the Long Term Evolution generation) means introducing all security threats and vulnerabilities of Internet to cell phone networks.

There are many new techniques for wireless transmission, for example: beamforming, cooperative beamforming, subcarrier allocation, cognitive radio technology, Orthogonal Frequency Division Multiple Access, new bands for data transmission (e.g. Extra High Frequency), Near Field Communication, Visible Light Communication, acoustic channel communication, handover processes, mesh networks and cooperative relaying, mobile IPv6, cloud-managed WLANs, out-of-band authentication systems.

All these qualitative and quantitative changes have significant impact on data transfer functionality and security – these two features of IT systems should be evaluated together, the trade-offs between them should be carefully considered [2]. It is an important question if all the old-style network security technologies can keep up with the changes of network environment?

Every new communication mode, new application, new technique mean novel software. Innovative software means software that is not matured, software full of vulnerabilities, software that makes it much easier to attack the particular part of the system. The problem should be analysed from many viewpoints.

New classes of threats

Another important topic is related to new classes of threats and attacks that materialize in information and telecommunication environment. Let us mention just some of them: counterfeited hardware, malware integrated with hardware, fake base stations and fake access points in wireless communication systems, watering hole attacks, custom malware, advanced persistent threats (APT), fraudulent digital certificates (e.g. DigiNotar certificate authority breach in 2011), malware attack on BIOS and air-gapped system hacking techniques.

Threats are getting more targeted, voluminous and sophisticated (a malicious program called Flame[1] was discovered after evading detection by antivirus software for about 2 years) while networks grow more complex with the addition of more users, devices, traffic, etc. Let us mention just one example of voluminous attack – Heartbleed discovered in 2014 and connected with OpenSSL library. It was estimated that the bug could threaten about 17% of the Internet secure web servers[2]. The consequences of failing to protect systems have increased. The consequences may be of financial fraud but they may have also an impact on the reliability of critical infrastructure and even national security. Cryptography keys and certificates become stolen and sold on the underground marketplace. Stolen keys and certificates allow to breach even the most security conscious organizations and to increase the effectiveness of targeted phishing attacks.

Different, new forms of attack emerge with decrease in hardware cost. Some of the attacks were too expensive in the past. Today they are possible. An example is an attack based on creating a fake base station or a fake access point (with estimated hardware and software cost under a boundary of $1000) that has a stronger signal than a legitimate one (attack known as evil twin or IMSI-catcher, IMSI – International Mobile Subscriber Identity). Mobile devices are usually designed to connect to the station with the strongest signal, so they choose fake station instead of legitimate one. When the device associates with the fake station eavesdropping and other forms of security violations become possible.

[1] http://www.wired.com/2012/05/flame/

[2] http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

Network evolution leads to the situations in which well protected and poorly protected devices and systems are interconnected. Of course, the system is as hard as its weakest link. Watering hole attacks are a variant of pivot attacks, in which an attacker is able to pivot from low security target system (the initial victim) to another high security target system (the intended target). The attacks utilize the growing number of interconnections and growing number of devices within IoT. The low-security targets could be business partners, vendors with connections to enterprise networks or even the unsecure wireless network of a local coffee shop near the target. Due to widespread usage, these low-security targets might also be whitelisted or preapproved in the targeted enterprises or in their various security tools – they become backdoors to the protected system.

APT is long-term (some identified attacks lasted several years) attack performed with many, different hacking tools and methods. APT may incorporate the changes to system data that are so subtle they are not easily detectable by common intrusion detection systems (IDS). On the other hand, the unnoticeable manipulations to data processing systems may have substantial impact on business decisions.

Malware attack on BIOS (Basic Input Output System) allows arbitrary writes to the BIOS bypassing the existing low level protection that prevents reflashing of the BIOS firmware. Infecting this part of software is especially dangerous since the malicious code may remain undetected by antivirus protection and may live in attacked machine even after reinstallation of the operating system [12].

A simple method for protection against network attacks is an air-gap boundary – protected computer is unconditionally isolated from other computers and networks. Air-gapped systems are used in many places, e.g. in: classified military networks and industrial control systems that operate critical infrastructure. It seems that the air-gap protection is 100% attack-proof, but it isn't. It has been demonstrated that it is possible to retrieve data from an air-gapped computer and to send commands to the computer by many ways (with a use of so called hidden or cover channels): using heat emissions and built-in thermal sensors, using acoustic inaudible channels, using optical and electromagnetic channels (e.g. leaking electromagnetic emanation in the form of radio signals generated and transmitted by graphic card) [18].

We are just starting to understand all new threats that we are being exposed to. It is very important to understand all the security issues of network evolutions and to be aware of new threats related to malware and network evolution. At the same time we have to look for new opportunities for data protection and to incorporate these opportunities to modern networks.

Complexity of security tools

There are many different protection tools and methods used by organizations: different forms of firewalls, virtual private networks, IDS, IPS (Intrusion Prevention System), network proxies, antiviruses, malware sandboxes and so on. The problem is the tools and methods are frequently independent, the policies and rules related to each tool are overlapping. Such complex protection system was acceptable many years ago. Today, it means many challenges to network security staff. There are examples showing that the old, disconnected security controls are becoming less effective in the case of targeted, sophisticated threats and advanced malware. Independent security controls usually have some holes that may be exploited by sophisticated attacks.

Tens of thousands new malware are detected per day. Similar number of antimalware signatures is generated by antivirus vendors. When a new file in a user machine is processed by the antivirus system it is cross-referenced against all the signatures. One of the impediments in this case is network bandwidth. Antivirus vendors usually cannot afford to send a full set of signatures to every customer. As an alternative, they try to predict the signatures most likely to trigger an alert on client side. The problem is if the predictions made by vendors are correct. It is possible that customer using antivirus protection gets infected with malware that is already known to the vendor that should protect a given customer. Another problem is, that sometimes, the signatures are released to customers after several days. Such delayed protection is often ineffective since lifetimes of malware is usually very short. It is estimated that about 75% of all threats are seen only once or are seen throughout a day or two.

All these issues are accompanied by general shortage of security professionals. Security staff hiring challenges have worsened over the last several years. Companies throughout the World are working harder to find, hire and retain experienced security professionals. It is estimated that hundreds of thousands IT security professionals are required today.

Common network security based upon dedicated devices, manual processes require advanced security skills. They can't compete with the volume, variety and sophistication of modern forms of attacks. A gap between threats and protection widens in time. It may be assumed that cyber threats are growing exponentially as a function of new technologies and advances in exploit techniques. At the same time research and implementations in IT security provide just small increments in protection features.

IPv4/IPv6 Transition

Protocol transition in internetwork layer is the biggest and most complex transformation in Internet. The process started about 15 years ago and will continue for many years. It is not limited to IP version change. A lot of communication protocols, among them routing protocols (Border Gateway Protocol, Multiprotocol Border Gateway Protocol, Open Shortest Path First, Intermediate System – Intermediate System, Routing Information Protocol), management protocols (Internet Control Message Protocol, Domain Name Services) are already upgraded or need to be modified or upgraded in the future. There are many tunnelling/interoperability methods for the long period of IPv4/IPv6 coexistence: dual-stack architecture, 6to4, Teredo, ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), tunnel broker, 6RD, MPLS (Multiprotocol Label Switching), 6PE [3].

IPv6 was designed to solve some problems related to IPv4. IPv4 has many security drawbacks and IPv6 has to eliminate them. IPv6 provides integrated confidentiality, integrity and authorization. Nevertheless, there are many security issues linked to the transition. They are related to the transition process and to the new features of IPv6. Some of the issues are:

- first software implementations of new services (e.g. DNS for IPv6) are usually error prone [16],
- IPv6 jumbograms may be used to execute DoS (Denial of Service) attacks [7],
- IPv6 mobility feature may be exploited in some new forms of attacks [17],

- problems related to IPv4/IPv6 tunnelling (e.g. packet filtering in the case of double IP headers, IPv6 used as a covert channel) [8],
- problems related to dual-stack devices [4],
- privacy risks related to IPv6 address auto configuration,
- IPv6 addressing system makes vulnerability assessment harder, ranges of addresses are more difficult to scan,
- problems with firewall filtering rules related to pseudorandom, dynamic IP addressing mode of operation.

IoT and BYOD

There are many security related challenges associated to such modes of operation as IoT, BYOD and BYOW. It is estimated that there are now many times more mobile devices than PCs in the world. Sometimes, mobile devices are becoming the only way most users connect to the Internet. The problem is that security remains out of significance for typical mobile device user.

Furthermore, innovative consumer-grade mobile devices used in the BYOD manner are usually not included in centralized IT management and protection initiatives. At the same time, they become an important part of corporate networks processing sensitive data.

Such devices as smartphones and tablets used for years are already incorporated into management structure. The devices utilize extremely unreliable business applications inside the security perimeter of corporations. The applications that are often free or very cheap have a lot of software vulnerabilities. The applications have an access to sensors integrated with a given device and to other resources of the device. The applications are habitually not patched by their authors. Program writer priority is given to speed-to-market and user experience – the security is treated with low priority. It is estimated that more than 80% of smartphones remain unprotected from malware and attacks [15].

Furthermore, it must be noted that modern mobile devices offer growing functionality, they are usually integrated with many sensors: gyroscope, microphone, camera, accelerometer and GPS receiver. It was demonstrated several times that the sensors may be used for data security violation. For example, gyroscope may be used for eavesdropping [14], accelerometer data may be used for user identification [5]. During installation process unaware users give permissions to use the sensors to the third party applications. The permissions may be abused during normal operation by the applications.

It may be noted here that the problem is known to operating systems makers. For example, the newest version of Android operating system called Android M will include finer controls for users to choose what permissions applications have to access and collect data. The system is designed to enable users to choose what data and what sensors to allow third-party applications on an ongoing basis instead of live with the default permissions accepted at installation process. The post-installation controls for application permissions is probably the most significant development in making Android more secure.

IoT is a relatively new idea. It is assumed, that in the future many other devices will be connected to private networks: webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales, garage door openers, charging stations for electric cars, air condition systems, fitness monitors, devices to monitor and control home security systems, smart TVs and smart watches and many others. All the devices include mobile applications that can be used to access or control the devices remotely. Some of these devices have not one but many network interfaces (e.g. with different radio bands and different data link layer protocols).

Similar mobile devices, for example tablets, are used for years. The important difference between tablets and other things connected to Internet is much greater diversity of the new Internet connected items – network stack and the number of supported operating systems is more varied. It is expected that the devices will be produced by many thousands of manufacturers – very probably some of them without necessary staff with basic IT security background.

The IoT devices are so called low-security targets, they usually provide fewer safeguards and far less visibility into their internal settings and mode of operation, they are usually out of control of enterprise IT management. It is probable that none of these devices will connect to enterprise authentication systems and will integrate with existing patch management and access control systems. So, the devices may provide new entrances into internal infrastructure. If the attacks use compromised devices as a launch platform (e.g. for DDoS), they are very difficult to distinguish from valid requests and very difficult to defend. For example, according to HP report up to 70% of IoT devices do not use encrypted mode of communication. Smart TVs and other network aware gadgets routinely use short (e.g. 4 characters long) passwords, making it possible to successfully perform brute force attacks [10].

We had already seen network breaches of this kind. For example, in 2013 Target's network has been breached (with about 40 million debit and credit cards stolen) not directly but indirectly via its heating and ventilation system. The attack has been performed with a use of a new type of malicious software called memory-scraping malware[3]. Another example of such breach has been demonstrated in 2014. A number of network-connected security cameras with Universal Plug and Play (UPnP) protocol were breached giving attackers access to corporate networks. These infected cameras were used to scan for other network-connected devices[4].

Proper installation, network segmentation and testing of these devices will be critical. The processes have to be developed to scale.

IoT device usually means limited resources (computation power, memory, energy) in the devices. The limitations make it hard to implement strong security controls. IoT means also a lot of new communication protocols with new implementations, e.g.: Data-Distribution Service, Message Queue Telemetry Transport, Constrained Application Protocol, Extensible Messaging and Presence Protocol, Advanced Message Queuing Protocol. The protocols are relatively fresh and their implementations are vulnerable to common communication threats.

Cloud computing, cloud storage

Cloud computing is very complex, multifaceted mode of data processing based on resource sharing. Clouds are built with a use of many different technologies: communication protocols, network devices, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. All the security vulnerabilities of technologies enumerated above are applicable to cloud computing. Instead of cloud we may say Internet. So all the security issues related to the Internet are

[3] http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html

[4] http://rt.com/usa/vulnerable-hackers-security-internet-189/

essentially associated with every cloud computing system [11].

Furthermore, the security problems related to clouds are similar to those related to BYOD – organizations using the technology lose control over the parts of the entire computer systems (especially in the case of public or hybrid cloud model). They don't manage the resources that are accessed in the public, shared by many users cloud. They don't even know when the resources are accessed, by whom and from where.

Cloud services are also a new potential tools for malicious users. The cloud with big memory and a lot of computing power may be used to break an encryption key in the case the key is too difficult to break it on a standard computer. Clouds may be also used to launch DDoS attacks.

Another feature of clouds is multitenancy related to resource sharing and object reusability. Cloud computing model is based on resources (such as memory, programs) that are shared by many users/clients of a given public cloud provider. The users are separated at a virtual level, at the same time they are not separated at the hardware level. Multitenancy may be used to violate data security. For example, objects (like memory blocks, disk space) which are used consecutively by two different users create a potential confidentiality violation point. The second user may have access to data remaining in the object after the first user released the object. The confidentiality may be violated unintentionally or intentionally – representative hacker may demand a large amount of disk space and after granting the space he may look for sensitive data left by the previous user of the same disk area [20].

Clouds based model of computing is relatively immune to DoS attacks. It is assumed that a cloud provider may offer extra resources to absorb the additional load during the attack. Nevertheless, DoS (or DDoS) attack that is blending itself with normal requests is much more difficult to detect and to block. Furthermore, the additional resources accessed during an attack may cause significant financial burdens to corporations that come under attack.

The key ingredient of any secure system is separation. It is based on the ability to create boundaries between those parts of the system that must be protected and those that cannot be trusted. In the cloud computing model it is very difficult to specify if a cloud (particularly public one) is inside or outside the secure and trusted system. It is hard to draw the separation line.

Software Defined Networking

It is observable that old-style network security technologies can't keep up with some network evolutions including: virtual machines, cloud computing, network convergence, data replication services and user mobility. One of the prospective solution to the problem is already available – Software Defined Networking (SDN). SDN is defined as flexible, centralized, dynamic and software based network management system. SDN user/manager is generally not limited by network hardware properties that are built in by manufacturers. In the case of SDN the network devices (switches, routers, proxies, firewalls) are managed with a use of SDN domain controller – it is said that the data transfer plane is separated from the control plane.

It seems, that SDN has the potential to deliver real network security value. Generally, SDN centralization helps to centralize network security service policy and configuration management. SDN makes much easier to automate network violations detection and remediation. With a use of SDN idea it should be more natural to block malicious traffic in every device of the system or to separate the device which has been cracked. SDN solves the problem of network segmentation with potential high level of granularity – micro segmentation of network becomes possible. SDN may be utilize to mitigate cyber threats by allowing integrated countermeasures to be "piped in" to a communication path regardless of their physical location.

On the other hand, SDN may simplify attacks on networks. SDN means centralized management and the centralization is a drawback of the solution. SDN domain controllers (in the form of applications) that are used to manage network devices are built on general purpose computing platforms. The diverse security problems of these platforms are widely known. If a domain controller becomes compromised it may be used to violate the security of the whole network that is managed by this particular controller. All common security violations are possible: eavesdropping, MitM (Man in the Middle), spoofing, transfer analysis, DoS, route changes, malware injection. The possibility of such attacks has been demonstrated for OpenFlow, which is *de facto* standard protocol used for SDNs deployment [6, 13].

Wireless transmission

There are many new techniques for wireless transmission. Some of the key innovative techniques are: beamforming, cooperative beamforming, subcarrier allocation, Orthogonal Frequency Division Multiple Access (OFDMA), new bands for data transmission (e.g. EHF), Near Field Communication (NFC), Visible Light Communication (VLC), handover processes, mesh networks and cooperative relaying, mobile IPv6, cloud-managed wireless LANs, pre-authentication, imprinting, out-of-band authentication (e.g. VLC, NFC, Loud&Clear, Seeing-is-Believing). The techniques are not matured and should be implemented very carefully. Furthermore, commonly used in wired networks security controls such as EAP (Extensible Authentication Protocol) or Kerberos may be applied to wireless systems. Nevertheless, they should be revised and modified in order to adjust them to distinct features of wireless communication environment.

It is obvious that cryptography is very important security area. On the other hand, wireless environment is a system exemplifying some drawbacks of cryptography[5]. Representative mobile devices have relatively low processing power and memory, have internal power sources with restricted amount of energy. The factors limit the usage of advanced encryption algorithms. Encryption key distribution and other encryption related management processes become significant burden for the devices. It may be easily demonstrated how the processes degrade the device performance (e.g. reduce battery lifetime). Some modules of cryptography protection may be replaced by physical layer security controls. Techniques such as MIMO (Multiple Input Multiple Output), beamforming, OFDMA are widely adopted in modern wireless communication systems. In such systems eavesdropping risk may be minimized with a use of such methods as dedicated subcarrier allocation in OFDMA, transmit antenna selection and selective jamming [1].

Cognitive radio is a transmission system with the artificial intelligence support to learn and communicate with the surrounding environment so as to perceive the available electromagnetic spectrum in the space, limit and reduce the risk of occurrence of interferences. The technology is

[5] Even, fathers of cryptography indicate that "*cryptography is becoming less important*" – Adi Shamir, http://www.theregister.co.uk/2013/03/01/post_cryptography_security_shamir.

developing quickly because of the intensifying shortage of wireless spectrum resources (it is almost certain that IoT will have significant, negative impact on the shortage). Some new threats in cognitive radio systems have already been identified, among them: primary user emulation attack, primary user interference, data tamper attack of spectrum sensing, learning threats, artificial intelligence parameters threats. Some of the threats are related to dynamic spectrum access, others are related to artificial intelligence behaviour [19].

Conclusion

Data security is multifaceted problem. Increased complexity of computer networks means that it is more and more difficult to understand technology issues of the systems. Even though we well recognize technology we may not stop here the evaluation of the security. The work is to be done by many different actors: users, enterprises, researchers, governments.

Evaluating data security of the existing systems and designing new systems we have to incorporate not only technological aspects of the systems but also social, legal and organizational aspects. For example, large enterprises should invest in technical protection but at the same time they should transform their structures – for instance cybersecurity leadership in an enterprise should be divided into two people: one with business background, the other with information security background.

It is not possible to stop the progress of computer networks. It is not possible to stop the growth of functionality. But developing and changing IT concepts one has to carefully consider many trade-offs between functionality and security. In general, more functionality means less security. The consequences of failing to protect systems have increased. The consequences may be of financial fraud but also they may impact the reliability of critical infrastructure and even national security.

In almost all innovative technologies we observe user mistakes (related to security, e.g. short passwords, lack of encryption, lack of software upgrading) that are already known, mistakes that were frequently done in the past, mistakes that should be omitted.

Organizations which handle credit card transactions in real world are required to formally conform to PCI (Payment Card Industry) standards. Similar requirements should be introduced to virtual/network world. For example, certificate authorities should conform to minimum level of security. The level compliance should be audited by independent organization.

The innovative technology and innovative modes of operation (e.g. BYOD, clouds and other forms of services outsourcing) deteriorate the perception of perimeter security – level of protection on a virtual borderline between inner IT system and outside environment. Usually, any connectivity to systems or organizations outside of an organization provides an opening for unauthorized entities and security controls are deployed on the boundary. In a cloud computing model, the perimeter becomes indistinct, controls on the boundary become to some extent worthless. So, we have to design not only new tools but also new models of security.

From the data security point of view it seems appropriate to improve work with existing technology instead of looking at new, unconfirmed technologies that may further complicate network defences. Further research in the area is necessary. The work is necessary not only in the technological aspects of data security. Some new legal requirements are necessary. For example, data breach notification is mandatory for American corporations in many US states, at the same time European Union waits for similar law.

***Author**: dr inż. Tomasz Bilski, Politechnika Poznańska, Instytut Automatyki i Inżynierii Informatycznej, ul. Piotrowo 3a, 60-965 Poznań, E-mail: tomasz.bilski@put.poznan.pl.*
The work is supported by research project 04/45/DSPB/0136.

REFERENCES

[1] Bilski T., New Threats and Innovative Protection Methods in Wireless Transmission Systems, *Journal of Telecommunications and Information Technology*, National Institute of Telecommunications, Warsaw, No. 3/2014, s. 26-33
[2] Bilski T., Security-Functionality Tradeoffs in IP Transition Phase, *The 6th International Conference for Internet Technology and Secured Transactions* (ICITST-2011), December 11–14, 2011, Abu Dhabi, UAE (CD), 632-638
[3] Bilski T., From IPv4 to IPv6 – Data Security in the Transition Phase, *ICNS 2011: The Seventh International Conference on Networking and Services*, (Eds. J.M. Mauri, S. Fries, M.L.M. Lopez, R.J. Kovac), IARIA, Venice/Mestre, 66-72
[4] Cho K., Luckie M., Huffaker B., Identifying IPv6 Network Problems in the Dual-Stack World, *SIGCOMM '04 Network Troubleschooting Workshop*, Portland, USA, 2004
[5] Day S., et al., AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable, *NDSS '14*, 23-26 February 2014, San Diego, USA, http://synrg.csl.illinois.edu/papers/AccelPrint_NDSS14.pdf
[6] Francois J., et al., Network Security through Soft-ware Defined Networking: a Survey, *IIT Real-Time Communications (RTC) Conference - Principles, Systems and Applications of IP Telecommunications (IPTComm)*, Sep 2014, Chicago, United States, ACM
[7] Frankel S., Graveman R., Pearce J., Guidelines for the Secure Deployment of IPv6, *NIST*, 2010
[8] Hoagland J., The Teredo Protocol: Tunneling Past Network Security and Other Security Implications, *Symantec*, http://www.symantec.com/avcenter/reference/Teredo-Security.pdf, 2007
[9] Huston G., What's So Special About 512?, The Internet Protocol Journal, Cisco, De-cember 2014, 1-18
[10] Internet of Things Research Study 2014, *HP Development Company*, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf, 2014
[11] Inukollu V.N., Arsi S., Ravuri S.R., Security Issues Associated with Big Data in Cloud Computing, *International Journal of Network Security & Its Applications (IJNSA)*, Vol.6, No.3, May 2014, 45-56
[12] Kallenberg C., et al., Defeating Signed BIOS Enforcement, *MITRE Corporation*, 2014, http://www.mitre.org/sites/default/files/publications/defeating-signed-bios-enforcement.pdf
[13] Klöti R., et al., OpenFlow: A Security Analysis, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6733671, 2013
[14] Michalevsky Y., et al., Gyrophone: Recognizing Speech From Gyroscope Signals, 2014, https://crypto.stanford.edu/gyrophone/files/gyromic.pdf
[15] Mobile Security: BYOD, mCommerce, Consumer & Enterprise 2013-2018, *Juniper Research 2013*, http://www.juniperresearch.com
[16] Morishita Y., Jinmei T., Common Misbehavior Against, DNS Queries for IPv6 Ad-dresses, *IETF*, RFC 4074, 2005
[17] Nordmark E., Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC 4213, *IETF*, 2005
[18] O'Malley S.J., Choo K.R., Bridging the Air Gap: Inaudible Data Exfiltration by In-siders (May 1, 2014), *20th Americas Conference on Information Systems (AMCIS 2014)*, 7-10 Aug. 2014, Association for Information Systems, Forthcoming. Available at SSRN: http://ssrn.com/abstract=2431593
[19] Tang L., Wu J., Research and Analysis on Cognitive Radio Network Security, *Wireless Sensor Network*, 2012, 4, 120-126, http://dx.doi.org/10.4236/wsn.2012.44017
[20] Zissis, D., Lekkas D., Addressing cloud computing security issues, Future Generation Computer Systems, *Elsevier*, 2012