ВЕЛИКОТЪРНОВСКИ УНИВЕРСИТЕТ
"СВ. СВ. КИРИЛ И МЕТОДИЙ"
ФАКУЛТЕТ "МАТЕМАТИКА И ИНФОРМАТИКА"

ЮБИЛЕЙНА МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ

50 ГОДИНИ ВТУ "СВ. СВ. КИРИЛ И МЕТОДИЙ"

СЕКЦИЯ
ФАКУЛТЕТ МАТЕМАТИКА И ИНФОРМАТИКА

10 МАЙ 2013 г.

АУДИТОРИЯ "ДЖОН АТАНАСОВ"

УЧЕБЕН КОРПУС 3

ГР. ВЕЛИКО ТЪРНОВО, УЛ. "АРХ. ГЕОРГИ КОЗАРОВ" 1, FMI@UNI-VT.BG

ПРОГРАМА
ЮБИЛЕЙНА МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ
50 ГОДИНИ ВТУ "СВ. СВ. КИРИЛ И МЕТОДИЙ"
СЕКЦИЯ ФАКУЛТЕТ МАТЕМАТИКА И ИНФОРМАТИКА

10 МАЙ 2013 Г.
АУДИТОРИЯ "ДЖОН АТАНАСОВ"
УЧЕБЕН КОРПУС 3

9:00 – 11:00	*Регистрация на участниците,* *Аула на ВТУ "Св. св. Кирил и Методий"*
11:00 – 12:00	*Пленарно заседание,* *Аула на ВТУ "Св. св. Кирил и Методий"*
13:00 – 14:00	*Регистрация на участниците,* *Аудитория "Джон Атанасов", учебен корпус 3,* *Ул. "Арх. Георги Козаров" № 1*
14:00 – 14:45	*In memoriam* *Аудитория "Джон Атанасов", учебен корпус 3*
14:45 – 15:00	*Кафе пауза*
15:00 – 18:00	*Заседание на секция 8. факултет "Математика и информатика"* *Аудитория "Джон Атанасов", учебен корпус 3*
19:00	*Коктейл: Интерхотел „Велико Търново"*

ПРОГРАМА НА ДОКЛАДИТЕ
ЮБИЛЕЙНА МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ
50 ГОДИНИ ВТУ "СВ. СВ. КИРИЛ И МЕТОДИЙ"
СЕКЦИЯ ФАКУЛТЕТ МАТЕМАТИКА И ИНФОРМАТИКА

час	***Автор, ЗАГЛАВИЕ***
	In memoriam
14:00 – 14:15	***Доц. д-р Маргарита Върбанова, проф. д-р Здравко Лалчев,*** Проф. дпн Иван Ганчев – създател на Методика на обучението по математика във Великотърновския Университет "Св. Св. Кирил и Методий"
14:15 – 14:30	***Доц. д-р Милко Такев,*** Акад. Борислав Боянов – Търновец, математик и родолюбец
14:30 – 14:45	***Проф. дмн Стефка Буюклиева,*** Учителят Стефан Додунеков
14:45 – 15:00	**Кафе пауза**
15:00 – 15:15	***Prof. Dr Andre Govaert,*** Improving Quality of Study Programmes. How Can we Improve the Learning Outcomes
15:15 – 15:30	***Нанко Бозуков,*** Информационна технология за енергийно спестяване при обновяване на сгради
15:30 – 15:45	***Стефка Буюклиева, Душан Биков,*** Wireless Network Security and Cracking Security Key
15:45 – 16:00	***Валентин Бакоев***, Комбинаторни и алгоритмични свойства на N-мерния булев куб
16:00 – 16:15	***Златко Върбанов, Тодор Тодоров,*** On DNA Codes and their Applications
16:15 – 16:30	***Златко Върбанов, Петя Белева-Димитрова,*** Процеси в ОС Windows и компютърни вируси
16:30 – 16:45	***Марияна Николова***, Проектите като образователна технология в обучението по информационни технологии
16:45 – 17:00	***Стефан Калчев, Васил Милев***, Архитектура на данните, фундамент на архитектурата на предприятие
17:00 – 17:15	***Силвия Върбанова***, Проектиране на уеб базирана информационна система за академичния състав на университетска катедра
17:15 – 17:30	***Камелия Колева,*** Синергетичните идеи при решаване на логически задачи
17:30 – 17:45	***Силвия Върбанова, Душан Биков, Верица Йовановска, Александър Кръстев,*** Costs And Investments Of Information Systems in Small & Medium Enterprises
17:45 - 18:00	***Димо Милев*****,** Методи за изследване на информационни системи
18:00 - 18:15	***Гергана Маркова,*** Анализ на подходите за сегментиране при разпознаване на символи
18:15 - 18:30	***Тихомир Трифонов, Георги Димков, Иван Симеонов***, Визуализации на звук и комплексни числа

WIRELESS NETWORK SECURITY AND CRACKING SECURITY KEY

Dusan Ilija Bikov, Stefka Hristova Bouyuklieva, Aleksandra Ilo Stojanova

Abstract

Wireless technology gives us mobility easy access to the computer network without copper wires. With the increased use of wireless technology, more and more Wi-Fi hotspots, rising number of cell phones, PDAs, Tablet PC, laptops (devices with Wi-Fi module), wireless security is an ever increasing issue for many organizations. In other words wireless networks add another entry point into a network for hackers. Because this technology is relatively new there is many security vulnerabilities.

In this paper, we study security on the wireless network and its vulnerability, also we give examples of how hackers can crack security key*, explode vulnerabilities and attack the wireless network. We consider the weak points of these networks in order to suggest ways and methods to ensure a good protection.*

Key words*: wireless security, key cracking, WEP, WPA/WPA2*

Wireless network security

Wireless network is a relatively new technology compared to wired network technologies and has fewer available security options. We can categorize security methods by the applicable layer of the OSI model.

Layer 2, or MAC layer, security options are as follows:	
Static WEP - Wired Equivalent Privacy (not recommended)	
Authentication type:	Shared Key Open System
WEP Key Format:	ASCII Hexadecimal - (0-9, a-f, A-F)

<table>
<tr><td>Key Type:</td><td colspan="3">64-bit, 10 hexadecimal digits or 5 ASCII characters
128-bit, 26 hexadecimal digits or 13 ASCII characters
152-bit, 32 hexadecimal digits or 16 ASCII characters
256-bit, 58 hexadecimal digits or 29 ASCII characters</td></tr>
<tr><td colspan="4">Is concatenated with a 24-bit initialization vector (IV) to form the RC4 key</td></tr>
<tr><td colspan="4">WPA/ WPA2(802.11i) - Wi-Fi Protected Access (Personal/Enterprise)</td></tr>
<tr><td>Wi-Fi Security</td><td>Authentication</td><td>Cipher</td><td>Encryption</td></tr>
<tr><td>WPA-Personal</td><td>Preshared Key</td><td>TKIP</td><td>RC4</td></tr>
<tr><td>WPA-Enterprise</td><td>802.1X/EAP</td><td>TKIP</td><td>RC4</td></tr>
<tr><td>WPA2-Personal</td><td>Preshared Key</td><td>CCMP (default)
TKIP (optional)</td><td>AES (default)
RC4 (optional)</td></tr>
<tr><td>WPA2-Enterprise</td><td>802.1X/EAP</td><td>CCMP (default)
TKIP (optional)</td><td>AES (default)
RC4 (optional)</td></tr>
<tr><td>Password (Passphrase):</td><td colspan="3">Hexadecimal, length between 8 and 64 characters
ASCII, length between 8 and 63 characters</td></tr>
<tr><td>Radius:</td><td colspan="3">WPA/WPA2 based on Radius Server</td></tr>
<tr><td colspan="4"><u>Layer 3, or Network layer, security options are as follows:</u></td></tr>
<tr><td colspan="4">IPSec - Internet Protocol Security</td></tr>
<tr><td colspan="4">SSL VPN (Secure Sockets Layer virtual private network)</td></tr>
<tr><td colspan="4"><u>Layer 7, or Application layer, security options are as follows:</u></td></tr>
<tr><td colspan="4">Secure applications such as Secure Shell (SSH), HTTP over SSL (HTTPS), and FTP/SSL (FTPS)</td></tr>
</table>

Table 1. Wireless network security

Nowadays wireless networking products are more prevalent and cheap and anyone can set up a WLAN for a few minutes (configuring is not always secure) [10]. This widespread use of wireless networks means many potential network intruders [12].

The following recommendations will improve the secure wireless network: change default administrator passwords and usernames, use WEP/WPA encryption, change the default SSID, do not auto-connect to open Wi-Fi networks, enable firewall settings on your laptop and home access point, reduce Wi-Fi transmitter power, disable remote administration.

Wired Equivalent Privacy (WEP)

WEP is a security algorithm for IEEE 802.11. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network [1]. WEP uses the stream cipher RC4 for confidentiality [2], and the CRC-32 checksum for integrity [3].

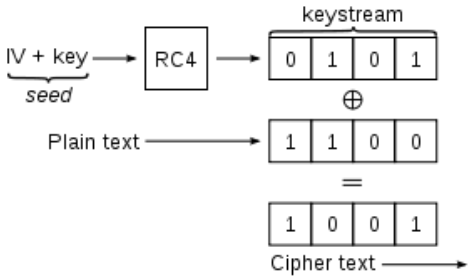

Fig.1. Basic WEP encryption: RC4 keystream XORed with plaintext

Standard 64-bit WEP uses a 40 bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key. Similarly we have 128, 152 and 256-bit WEP key, available from some vendors.

As there are serious security flaws in the protocol which lead to practical attacks demonstrating that WEP fails to achieve its security goals, new standards are developed.

WPA/WPA2

To fix the problems of WEP, a new standard with the name Wi-Fi Protected Access (WPA) was released in 2003. It is now a part of the IEEE 802.11 specifications [1]. WPA includes a message integrity check for prevent an attacker to capture, alter and/or resend data packets. The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP), was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change.

WPA2 also known as IEEE 802.11i-2004, is the successor of WPA. When 802.11i started winding down, the Wi-Fi Alliance updated the WPA standard to

WPA2. WPA includes a requirement for just TKIP encryption; WPA2 requires support for both TKIP and AES. Almost all gear shipped starting in late 2002 could be upgraded to work with AES [4,5].

Encryption protocols

TKIP (Temporal Key Integrity Protocol) uses RC4 as its cipher with a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. First, it implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization. Finally, TKIP implements a 64-bit Message Integrity Check (MIC). Key mixing increases the complexity of decoding the keys by giving an attacker substantially less data. The message integrity check prevents forged packets from being accepted. Under WEP it was possible to alter a packet whose content was known even if it had not been decrypted.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) uses a 128-bit encryption key and a 128-bit block size of data.

Wireless Hacking Techniques

Most wireless hacking attacks can be categorized as follows: Eavesdropping or Sniffing, DoS, AP Masquerading or Spoofing, MAC Spoofing, Planting Rogue Access Points, Cracking Encryption and Authentication Mechanisms. Here we will talk about Cracking Encryption and Authentication Mechanisms. Mechanisms include cracking WEP, WPA/WPA2 preshared key authentication passphrases. Hackers use these mechanisms to connect to the WLAN using stolen credentials, capture other users' data and decrypt or encrypt it.

Authentication and Cracking Techniques

Two methods of authentication can be used in the 802.11 standard: Open System authentication and Shared Key authentication.

Open system does not provide any security mechanisms, it is simply a request to make a connection to the network. Subsequently WEP keys can be used for encrypting data frames. At this point, the client must have the correct keys.

In shared-key authentication the client uses the WEP key for authentication in a four step challenge-response handshake. After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4. It is easy to obtain a plaintext/ciphertext pair by monitoring: the attacker learns both the cleartext challenge sent by the AP and the encrypted version sent by the client. From this, it is easy to derive the keystream used to encrypt the response [6].

RC4 is a stream cipher and the same traffic key must never be used twice. The purpose of IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network and there is 50% probability the same IV to be repeated after 5000 packets. The method, known as the Fluhrer, Mantin and Shamir (FMS) attack, uses encrypted output bytes to determine the most probable key bytes, resulting in a passive attack that can recover the RC4 key after eavesdropping on the network [9].

WPA Personal uses an ASCII passphrase for authentication. WPA Enterprise uses a RADIUS server [11] to authenticate users. WPA Enterprise is a more secure robust security option but relies on the creation and more complex setup of a RADIUS server.

Figure 2 shows the 802.1x/EAP process and the communication process which is used to authenticate a client using 802.1x/EAP.

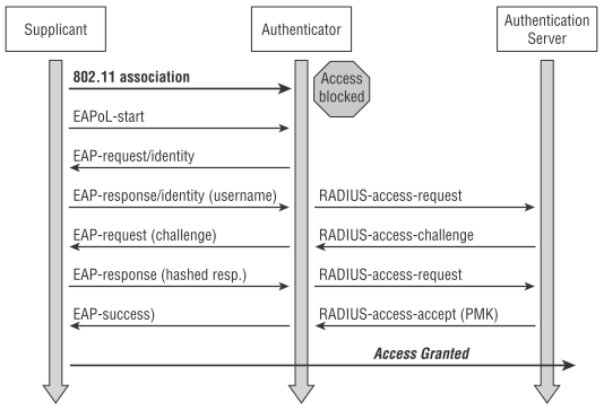

Fig. 2. 802.1X authentication process

802.11i and WPA use the same encryption and authentication mechanisms as WPA2. Table 2 summarizes the authentication and encryption options for WLANs and associated weaknesses.

	Encryption	**Authentication**	**Weakness**
Original IEEE 802.11 standard	WEP	WEP	IV weakness allows the WEP key to be cracked. The same key is used for encryption and authentication of all clients to the WLAN.
WPA	TKIP	Passphrase or RADIUS (802.1x/EAP)	Passphrase is susceptible to a dictionary attack.
WPA2	AES (can use TKIP while in mixed mode)	Passphrase or RADIUS (802.1x/EAP)	Passphrase is susceptible to a dictionary attack.
IEEE 802.11i	AES (can use TKIP while in mixed mode)	Passphrase or RADIUS (802.1x/EAP)	Passphrase is susceptible to a dictionary attack.

Table 2. 802.11 and WPA security solutions and weaknesses

Cracking WEP security key

We can easy crack WEP key, if we have compatible wireless adapter (Atheros, AirPcap, Wi-Spy, etc.) and keys cracking program (AirSnort, WEPCrack, Reaver, Aircrack, etc). Although a hacker can attempt to crack WEP by brute force, the most common technique is the FMS attack.

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks (statistical cracking method), as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools [8]. To crack the WEP we use aireplay-ng which replaies an ARP (address resolution protocol) packet to generate new unique IVs. To crack the WEP key for an access point, we need to gather lots of initialization vectors. Once we have captured a large number of IVs, we can use them to determine the key.

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng [8]. Some information from airodump-ng for the Test network is shown in Table 3.

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
B0:48:7A:AC:20:E4	-51	75	0	0	9	54e.	WEP	WEP	OPN	Test

Table 3. Airodump-ng in monitor Test network

Here are the basic steps we can use to determine the WEP key:

1. Test Wireless Device Packet Injection
2. Start airodump-ng to capture the Ivs
3. Use aireplay-ng to do a fake authentication with the access point
4. Start aireplay-ng in ARP request replay mode
5. Run aircrack-ng to obtain the WEP key
6. sudo aircrack-ng -K -b B0:48:7A:AC:20:E4 Wep_Test-01.cap

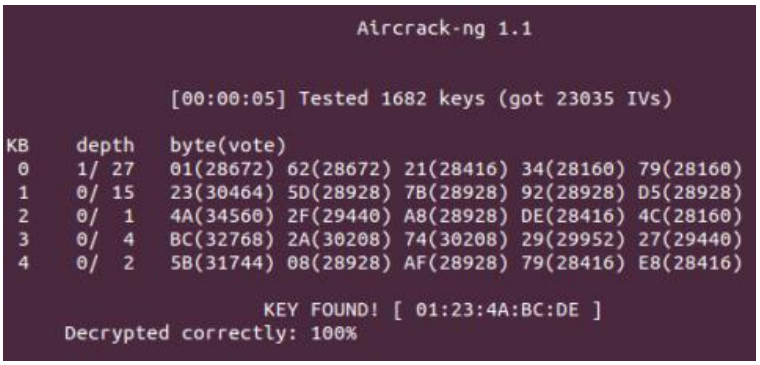

Fig. 3. Aircrack-ng crack WEP key

Depending on the type of the attack we need different number of IVs for cracking the key. With the option ”-K” we use FMS/KoreK (250,000 Ivs, 64 bit, etc.) attack, default type of attack for 1.0-rc1 is PTW (20,000 packets, 64-bit, etc.).

Cracking WPA/WPA2 security key

We can crack WPA/WPA2 key, but we need compatible wireless adapter and keys cracking program (Reaver, Aircrack, etc) and dictionary.

Aircrack-ng can only crack WPA/WPA2 pre-shared keys. The user has to be sure that the authentication type of network is PSK, otherwise, he can try to crack it. The only thing that gives the information to start an attack is the handshake between the client and AP. Four-way handshaking is done when the client connects to the network and messages (EAPOL-Key frames) are exchanged (fig. 4).

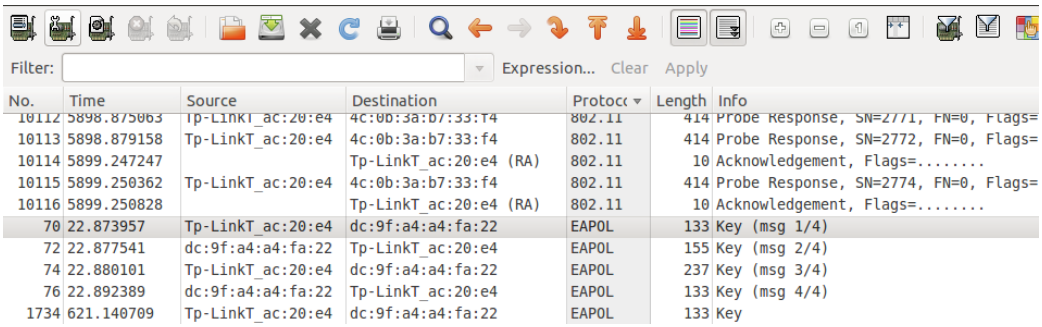

Fig. 4. Wireshark, show EAPoL packets

To have an unbreakable wireless network at home, one should use WPA/WPA2 password composed of random characters including special symbols [8]. If ASCII characters are used, the 256 bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1 [7]. To crack the key, it must be contained in the dictionary which is used for breaking the WPA/WPA2. There is no difference between cracking WPA or WPA2 networks.

Information from airodump-ng for the Test network is shown in Table 4.

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
B0:48:7A:AC:20:E4	-51	75	0	0	9	54e.	WPA2	CCMP	PSK	Test

Table 4. Airodump-ng in monitor Test network

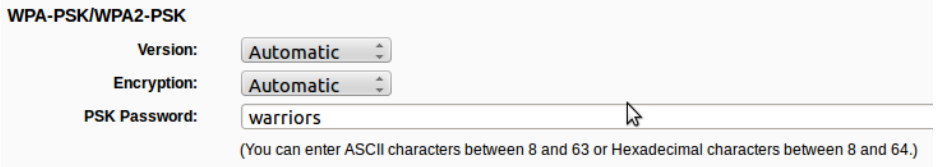

Fig. 5. AP interface for set the security key

Here are the basic steps for cracking WPA/WPA2 key:

1. start airodump-ng to collect authentication handshake
2. use aireplay-ng to deauthenticate the wireless client
3. run aircrack-ng to crack the pre-shared key
4. sudo aircrack-ng WAP_Test-01.cap -w password.lst

Figure 6 shows the result of the key cracking. We made a password list with hundreds of words and put the security key “warriors” on the list. There are ready-made dictionaries with several million words, and specifies dictionaries also can be generated.

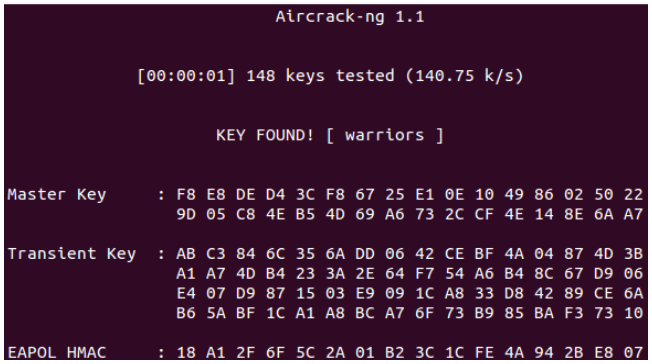

Fig 6. Aircrack-ng crack WPA/WPA2 key

Conclusion

The goal of this paper is to show some basic security methods, which can make the wireless network more secure. We can configure AP using techniques which improve the security. Here we show mechanisms for authentication of wireless networks, security solutions, weaknesses, etc.

To crack the wireless security key, the attacker must have compatible wireless adapter and keys cracking program. The using of WEP encryption is not recommended, because WEP key is easy to be cracked. On another hand WPA/WPA2 is more secure but is susceptible to a dictionary attack, and here we must use strong security key (number, character, special symbols).

REFERENCES

[1] IEEE-SA Standards Board. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Speci_cations. Communications Magazine, IEEE, 2007.

[2] Seth Fogie, "WPA Part 2: Weak IVs", in Security Reference Guide, informit.com. Last updated Dec 23, 2004.

[3] William Arbaugh, "An Inductive Chosen Plaintext Attack against WEP/WEP2". cs.umd.edu. May 2001.

[4] Glenn Fleishman, "Battered, but not broken: understanding the WPA crack". Ars Technica. 2008-11-06, http://arstechnica.com/security/2008/11/wpa-cracked/.

[5] Jakob Jonsson. 2002. On the Security of CTR + CBC-MAC. In *Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography* (SAC'02), K.Nyberg and H.Heys (Eds.). Springer-Verlag, London, UK, 76-93.

[6] Nikita Borisov, Ian Goldberg, and David Wagner. 2001. Intercepting mobile communications: the insecurity of 802.11. In *Proceedings of the 7th annual international conference on Mobile computing and networking* (MobiCom '01). ACM, New York, NY, USA, 180-189.

[7] Van Rantwijk, Joris (2006-12-06). "WPA key calculation — From passphrase to hexadecimal key". Retrieved 2011-12-24.

[8] http://www.aircrack-ng.org/

[9] Martin Beck and Erik Tews. 2008. Practical attacks against WEP and WPA. *Proceedings of the second ACM conference on Wireless network security* (WiSec '09) ACM, New York, NY, USA, 79-86.

[10] Neil Skea and Manoj Maharaj. 2011. Wireless Network Security. Alternation 18,1 (2011) 318 - 335 ISSN 1023-1757

[11] Iyad Aldasouqi and Walid Salameh. Detecting and Localizing Wireless Network Attacks Techniques. I*nternational Journal of Computer Science and Security*. ISSN 1985-1553Volume: 4; Issue: 1; Start page: 82; Date: 2010;

[12] Hongbo Liu, Hui Wang and Yingying Chen, Ensuring Data Storage Security against Frequency-Based Attacks in Wireless Networks, Distributed Computing in Sensor Systems, *Lecture Notes in Computer Science*, vol. 6131, 2010, pp 201-215.

PhD Student Dusan Iilija Bikov,
Department of Information technologies,
St.Cyril and St.Methoduis University of Veliko Tarnovo
e-mail: dule.juve@gmail.com

Prof. Stefka Hristova Bouyuklieva, Dr. Habil,
Department of Algebra and Geometry,
St.Cyril and St.Methoduis University of Veliko Tarnovo
e-mail: stefka@uni-vt.bg

Aleksandra Ilo Stojanova
Faculty of Computer Science, University "Goce Delcev" - Shtip
e-mail: stojanova_alex@yahoo.com