International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-3,March 2016
ISSN: 2395-3470
www.ijseas.com

Contemporary Research on Identity Theft Techniques used on Smart Devices

David Malanik[1], Roman Jasek[1]
[1] Faculty of Applied Informatics, Tomas Bata University in Zlín, Zlín, Czech Republic

Abstract
This paper provides a brief introduction concerning trends in modern security threats using online identities. The paper deals with two major modern-day facts: the first fact is the increasing number of active online smart devices; the second fact deals with economic impacts of identity theft, as shown in long-term studies. Many users save online identities in their smart devices. These devices provide improvements and simplify online activities, but very personal information is necessary to operate some types of online identities, which are then reconstructed from online profiles. Smart devices become the user's online identity, which is necessary to protect. However, smart devices provide only very basic and limited protection functions. If there is no security toolkit installed, it is very difficult to protect a user's online identity and identity theft operations become easier. The attacker only needs access to the victim's smart device. This paper shows techniques for infiltrating a victim's smart device and for stealing private data.
Keywords: *identity theft, smart devices, malware, hacking, security.*

1. Introduction

There are many users' identities on the internet. Many of these are dummy identities, but most are real identities. The problem lies in verifying these identities because internet identities do not contain verification procedures as State identities do [3]. For example, an identity on Facebook does not require any real personal information - just a valid e-mail address. Another problem is with e-mail accounts. Free mail checks take place only if an email with the same name does not exist. It is possible to use another person's identity because only a login name and password are needed to access the identity, and anyone can use any identity. It is very easy to use an alien identity and this can lead to identity thefts. Identity thefts represent one of the most important problems of the cyber world [7]. The statistics in the next parts of this paper prove just how profitable gaining personal information is.

The next evolution represents the increasing number of smart devices connected to the internet. One other factor increases the number of smart devices connected to the internet; it is the migration of virtual identities from computers to smart devices. The number of identities stored inside smart devices is increasing rapidly. They become very profitable targets for many attackers [9].

2. The increase of smart devices connected to the Internet

The number of smart devices increases every day, which many companies report. Fig. 1 shows the estimated number of smart devices in 2015 and for the next 3 years. There are more than 1.9 billion active smart devices in the world and this number shows how many potential attacks exist.

The next important breakthrough is the increasing number of wearable Hardware (HW). 'The Internet of Things' represents the next highly developed sector of smart devices that will be connected to the internet. This evolution transfers user cyber identities from personal computers to notebooks. The next step is to transfer cyber identities to smart devices (smart phones that have the HW specifications that computers had in 2010). Smart devices contain operation systems and operate as computers. This evolution transfers personal cyber identities to wearable HW and is bound to happen very soon.

The initial step of this evolution is shown in Table 1. This graph shows the increasing number of wearable HW worldwide. This signals an important evolutionary step, that wearable HW is suitable for many people and is demanded by consumers. The Gartner shows there were approximately 3.03 billion of these smart devices in 2013. In 2015 the figure is 4.9 billion. It is predicted that in 2020 there will be more than 25 billion smart devices worldwide.

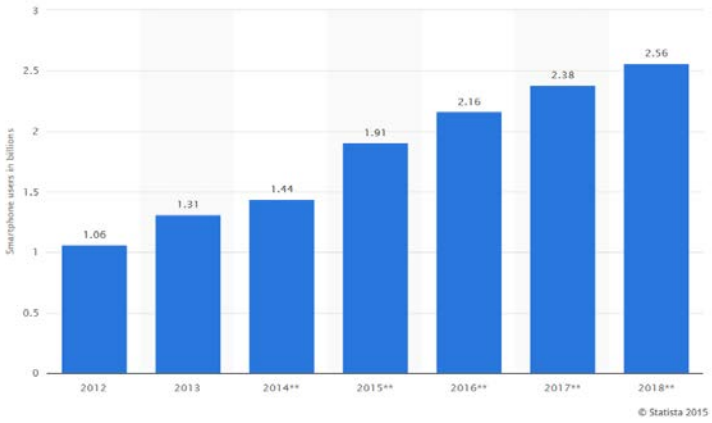

Fig. 1 Number of smart phone users [10]

The total number of wearable HW units is shown in the table below. There is a significant increasing trend here.

Table 1: Number of internet devices in units[11]

Category	**2013**	**2014**	**2015**	**2020**
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2,874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

3. Evolution of identity theft

United States Bureau of Justice statistics report significant increases in identity theft in the last few years. There is a continuous increase of households that were victims of identity theft, or victims of the misusage of personal information. The increase between 2005 and 2007 is shown in Table 2.

Table 2: Identity theft statistics 2005-2007[1]

	2005	2006	2007
Total number of identity thefts	6,424,900	7,864,400	7,928,500
Existing credit cards	2,971,900	3,623,700	3,894,300
Other existing accounts	1,585,500	2,086,500	1,917,000
Personal information	1,078,700	1,123,800	1,031,200
Multiple types	788,800	1,030,500	1,086,100

This increase continued in the year 2009 but in 2010 there was small decrease of identity thefts. The statistic shows the scatter of targets. The main target is the existing credit card in all year. This reflect the more profitable target for attackers.

Table 3: Identity theft statistics 2009-2010[2]

	2009	2010
All types of identity theft	8,890,000	8,571,900
Existing credit cards	4,986,500	4,625,100
Other existing accounts	2,202,500	2,195,900
Personal information	826,800	775,400
Multiple types	874,200	975,521

This next part of this paper results from the second analysis, performed in 2015. The number of theft incidents increased rapidly between 2010 and 2012 (from 8.5 million to 15.6 million) which is an 84% increase. The increase is shown in Table 4.

Table 4: Identity theft statistics 2012 and 2014[3]

	Number of victims	
	2012	**2014**
All types of identity theft	16,580,500	17,576,200
Existing credit cards	7,698,500	8,598,600
Existing bank accounts	7,480,700	8,082,600
Other existing accounts	1,696,400	1,452,300
New accounts	1,125,100	1,077,100
Personal information	833,600	713,000

[1] http://bjs.gov/content/pub/pdf/itrh0510.pdf

[2] http://bjs.gov/content/pub/pdf/itrh0510.pdf

[3] http://www.bjs.gov/content/pub/pdf/vit14.pdf

There is a significant increase of successful attacks on bank accounts between 2010 and 2012, from 2.2 million to 7.5 million. This reflects the trend of widespread cyber identities. There are many cyber identities associated with real bank accounts. The attack platform has changed from use of only credit cards to using credit cards plus bank accounts. Smart devices with internet banking applications will be very lucrative targets.

4. Mobile malware

There are a few techniques by which hiding malware applications are hidden inside Android devices. The techniques vary for the two major series of Android operation systems. The breaking point for techniques is the Android version 2.3.3, which introduces many improved security settings, and solves the Broadcast Receiver problem in older versions of Android. The perfect malware for mobile devices has a simple life cycle. The ideal life cycle is shown in Fig. 2.

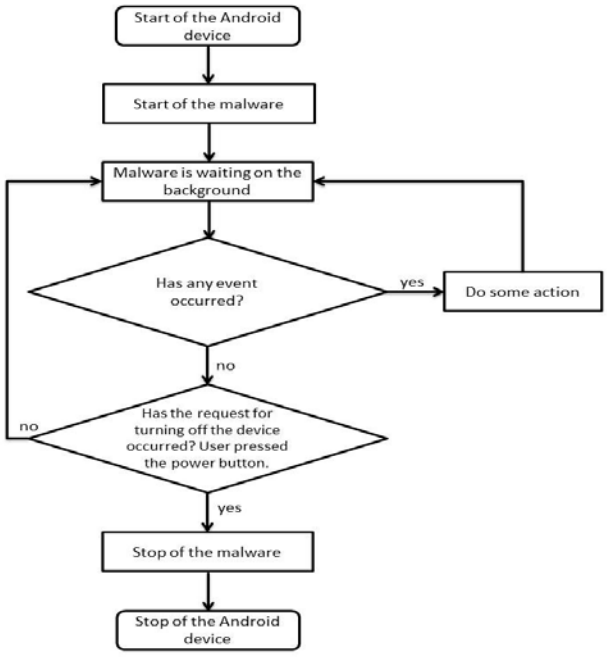

Fig. 2 The ideal life cycle of malware

4.1. Android OS version 2.3.3 and lower

The process of developing malware for Android 2.3.3 and lower versions is composed of the following steps: firstly, an Android project is built up, which is the same as a standard application project. Secondly, a sample of the Broadcast Receiver class is made and its method on Receive is implemented.
With the AndroidManifest.xml file, it is possible to assign it to receive SMS activity:

```
<receiver android:name=".MalwareReciever"
        android:exported="true"
        android:permission="android.permission.BRO
ADCAST_SMS">
        <intent-filter>
                <action
        android:name="android.provider.Telephony.S
        MS_RECEIVED"/>
        </intent-filter>
</receiver>
```

This provides the customer BroadcastReceiver, but this receiver is detectable in running applications. The next step is to provide covering operations for this. The first option is to use the specific name for the Activity (for example “Google Synchronize Android Service”). The second option comes from specific behavior of running application managers in old versions of Android. The application without running Activity is not shown in the running application manager. The malware has Activity assigned to receive SMS, so this is inactive until the smart device receives an SMS. Next, the malware captures data, processes it, and sleeps. It is detectable only for a very limited time.

4.2. Android OS version 3.1 and higher

This malware must be different to lower Android versions because the Google Incorporated Company (Google 2014) has improved security for these latest versions of Android that no longer allows the malware to silently execute its tasks only via BroadcastReceiver. Nowadays, if BroadcastReceiver requires permission, then each application with BroadcastReceiver must also have an Activity. The malware, developed as it was described above, can be successfully installed on devices running Android 3.1 or higher versions, but the application does not work. Here, however, is a solution.
Developing the malware here is the same, but the covering functioning malware in the running application manager must be different. The Activity is visible in the running application and it is essential to make the Activity transparent. This can be done by

editing the style in .../res/values/ styles.xml file, where we add these item tags:

<item name="android:windowIsTranslucent">true</item>
<item name="android:windowBackground">@android:color/transparent</item>
<item name="android:windowContentOverlay">@null</item>
<item name="android:windowNoTitle">true</item>
<item name="android:windowFullscreen">true</item>
<item name="android:windowIsFloating">true</item>
<item name="android:backgroundDimEnabled">false</item>

The Activity is now transparent, but the name of the Activity is still visible. The next step is to edit the file: .../res/values/strings.xml. The value must be changed from '<string name="app_name">Google Service Setup</string>' to '<string name="app_name">' </string>. Notice that the new value is not null, but it is a space. Next, it is essential to ensure that the parameter android:label of the application tag, which is in the AndroidManifest.xml file, refers to this value: android:label="@string/app_name". It is not a good idea to edit the parameter android:label directly in AndroidManifest.xml file. The next step is to replace standard icons with transparent PNG images. It is done in the directories: .../res/drawable-hdpi, .../res/drawable-mdpi, .../res/drawable-xhdpi and .../res/drawable-xxhdpi.

5. Identity theft scenario

The increasing number of smart devices brings one other associated factor - the need to connect these devices to the internet. Many applications need internet connection to function fully. Now, there are more smart devices that are always on-line with lower speed, and wireless hotspots in cities is also important for users.

The identity theft scenario described in this part shows a model situation in a rogue hotspot in the street. Components for this scenario are a wireless router with high operating system (it is almost impossible to perform this with a home AP), a USB LTE modem (or another equivalent connection to the internet) and also prepared malware for the targeted smart device. The Android platform is the target for this scenario, and due to the fact that we need to install the application from a rogue hotspot, iOS devices do not support software installation from other sources.

5.1. Rogue hotspot HW

The The HW part of the router is represented by the Banana Pi R1 device, which is derived from the more popular Raspberry Pi device. The big advantage of the Banana Pi R1 device compared to the Raspberry, is a 1 Gbit Ethernet port, dual core processor and a 1 GB RAM. The ARM device represents a flexible platform in order to implement many functions. It is possible to use the device for very sophisticated applications and /or attacks. A further benefit of this device is the low price, around 80 EUR (100 USD) (as of October 2015).

This device is quite small and it is possible to install this wherever the attacker chooses. The battery has a capacity of 10,000 mAh and is capable of running the device for more than 6 hours. The maximum power consumption of the Bpi R1 is approximately 2.5 W. Fig. 3 shows the device with attached Wi-Fi antennas:

Fig. 3 Banana Pi R1

Main advantages or reasons for choosing the Banana Pi R1:

- It is a small device, ideal for hiding installations
- It has a powerful HW - 2 core CPU, 1GB RAM, 802.11n Wi-Fi, and SATA HDD
- It has minimum power requirements

- It has an open OS system and it is possible to install any Linux ARM distribution
- It has a low price, about 100USD without HDD.

Internet connection for the victim

Connecting to the internet is possible in two main ways: the first way is to install a wired internet connection. This uses Ethernet ports for internet connection, but this solution is not good for smart mobile devices. The second way is by installing the mobile LTE modem, which uses an LTE modem connected to the USB port on the Bpi R1 smart device. The essential question in many identity attack scenarios is the cost of the attacks [6]. Table 6 shows scenario costs of attacking smart devices. These prices are valid for the Czech Republic and may be different in other countries. The currency converter calculates using the exchange rate of 23.9 CZK / 1USD (as of October 2015). The cost of attacks is very low.

Table 5: Cost of the solution

Device Bpi R1	*100 USD*
USB LTE modem	40 USD
LTE data tariff (FUP[1] 5GB)	20 USD/month
Summary	160 USD – first month
Periodical payment	20 USD/month

5.2. Attacking malware

This part refers to the previously described camouflage techniques from the Mobile malware chapter. The main goal is to install custom malware applications to the victim's device which have a legal frontend. The application is the mobile hotspot connector and contains two parts. The first part of the application is the true mobile hotspot connector and it provides covering operations for the malware part. The second part of the application provides the sniffing operation inside smart devices. The frontend of the application is shown in Fig. 4.

Fig. 4 Malware application frontend

The application successfully connects to the rogue AP. Without it, it is impossible to connect to the Wi-Fi network and so the application is necessary for internet access.

The second hidden part of the application operates in the background and captures all login credentials and personal information that the victim writes on the smart device. The sniffer is connected to three main processes: firstly, it is connected to the cyber keyboard process and provides standard key logger functions; secondly, it is connected to the screen process which supports key logger functions with screenshots. The last connection process is to the web browser, in order to sniff login credentials that the user provides on web pages. This solution captures login credentials for HTTPS pages.

The malware part of application communicates with the attacker in two possible ways. The first way is active while the victim is connected to a rogue AP in order to connect to the internet. This uses simple FTP protocol for uploading captured data directly to the rogue AP. All containers have the IMEI, name and IP of the victim device.

The second method uses other functions and it is active when the victim uses an internet connection in a place other than a rogue AP. This indicates the possibility that there is no FTP connection allowed on the victim's network. In this case, the application uses the HTTP GET request for a specific page by using encrypted captured data as the GET parameter [5]. The GET parameter must be divided into parts with a

[1] Fair User Policies - A download quota restricted by Internet service provider

maximum size of 2 KB (this limit is due to the specifications of HTTP). The always-working method, based on the http protocol and GET parameter, is shown in Fig. 5 [2,8].

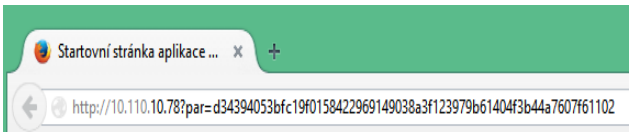

Fig. 5 Send captured credentials as the GET parameter

5.3. The attack process

This chapter describes the attack scenario, starting from the victim detecting the new wireless hotspot, to fully poisoned smart devices and successful identity theft. The basic attack scheme is shown in Fig. 6 below:

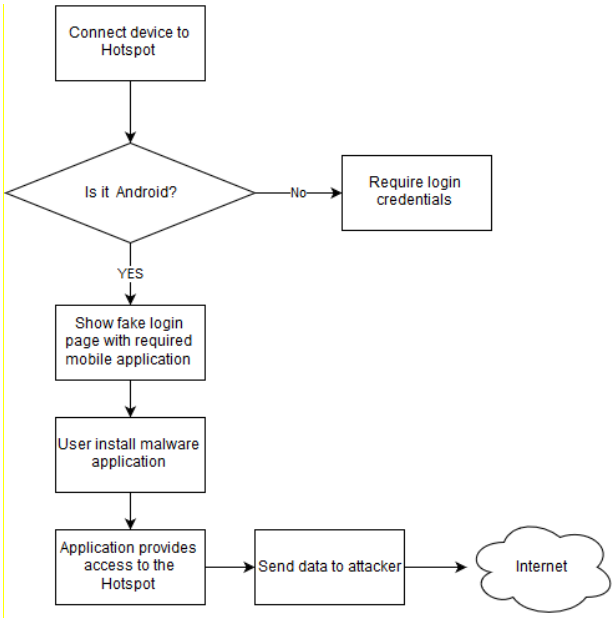

Fig. 6 Basic attack scheme

Firstly, the victim uses their smart device to connect to Wi-Fi. The smart device detects new wireless networks that do not have encryption, and informs the victim about it (Fig. 7).

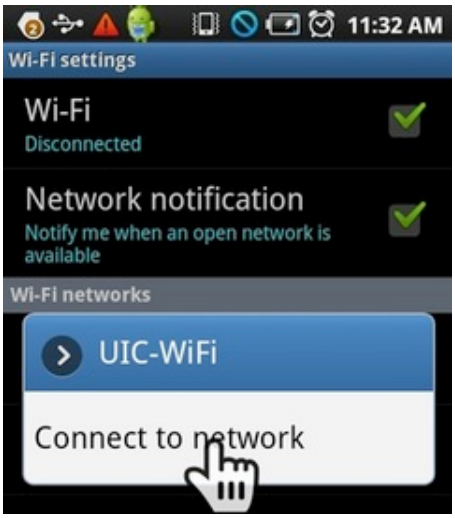

Fig. 7 New free Wi-Fi detected

The victim is redirected to the hotspot login page immediately after connection. The fake hotspot login page provides a simple choice - if the victim has an unsupported device (not an Android device), the login page requires the login name and password. Giving this information limits the number of potential victims, but the malware is not yet ready for other platforms. If the victim uses a smart device with Android OS, the login page requires a special application that connects to the hotspot infrastructure. The login page is shown in Fig. 8.

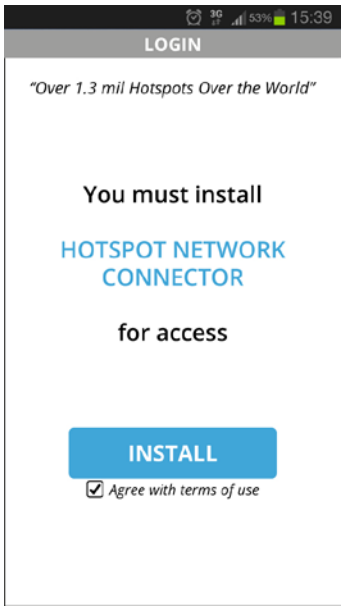

Fig. 8 Installing a hotspot application

This application requires the "necessary" permission in order to operate. The required permission is shown in Fig. 9.

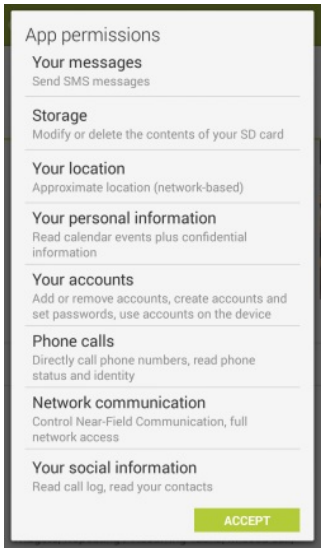

Fig. 9 Required permission for the malware application

The application is then successfully installed and provides access to the rogue AP, i.e. the fake hotspot. The victim obtains internet access. The price is interesting - just put all the credentials to the attacker AP.

Fig. 10 shows the file with captured login credentials. The file has a basic text format: the first part contains data carved from the application. The second part contains data carved from the web browser. There are various types of services (HTTP, FTP, ICQ, etc.), there are destination addresses (occasionally the login web page), a login name and a password.

```
IP: 192.168.123.10
IMEI: [redacted]
NAME: TestlabMP1
------------------------------------------------------------------------
APPLICATION
NAME                    DATA
------------------------------------------------------------------------
PayPal                  testl[redacted]      MPlabT[redacted]
Facebook                testl[redacted]      MPlabT[redacted]
Viber                   Meeting at PM5:45 at bus station :-D


------------------------------------------------------------------------
WEB BROWSER
SERVICE URI                             LOGIN                   PASS
------------------------------------------------------------------------
HTTPs   www.facebook.com                testl[redacted]         MPlabT[redacted]
HTTPs   www.ebay.com                    testl[redacted]         MPlabT[redacted]
HTTP    195.17[redacted]                testl[redacted]         MPlabT[redacted]
```

Fig. 10 Data from a victim‘s smart device

6. Conclusion

This continuing research shows the possibilities of advanced persistent threats of attack on smart (mobile phone) devices. Smart devices are vulnerable to these types of attacks, because few smart devices contain Antivirus solutions, and fragmented Android versions are not very effective. The primary target is the private identity from inside the smart device. The identity is represented by the login credentials for each service used by the victim. Social engineering techniques are used to poison the victim’s phone, which stems from the need to be online all the time. The main target user groups are those without mobile data connection, and who therefore search for free wireless hotspots. The solution is suitable for any cultural activity, such as festivals.

This paper documents the increasing number of smart devices and thus the increasing number of potential victims, and the increasing number of identity thefts in the last few years. The next question concerns the changes the new IoT[1] technology will bring. Many of the new devices require internet connection in order to work fully, and this number is increasing rapidly.

This situation does not have any simple solutions. The first problem stems from the human factor that people are not aware of such potential threats and type in too much personal information (including login credentials) into their smart devices. The chapter on smart device applications shows how more and more applications require internet access in order to fully function, thus increasing this problem.

The second problem is due to the Android platform. This platform is totally open, and it is easy to install and is from unknown sources. Many users install this application without realising the potential risk. The distribution of malware application is easier on Android OS than on iOS platforms.

It is necessary to totally change our stance on the security of smart devices. These are not safe mobile phones. These are computers with operating systems; they contain many vulnerabilities, both known and unknown, and they can be hacked into and an outsider can take control of them. The last question will be: “How easy is it to steal identities, and how profitable is the target?” These questions still remain between the attacker and the victim.

[1] Internet of Things

Acknowledgments

This work was supported by the European Regional Development Fund under the project CEBIA-Tech Instrumentation No. CZ.1.05/2.1.00/19.0376.

References

[1] Google, 2014 company, [online], https://www.google.com/about/company/.
[2] Jasek, R., Kolarik, M. & Vymola, T. (2013). APT Detection System using Honeypots. Proceedings of the 13th International Conference on Applied Informatics and Communications (AIC'13), WSEAS Press, pp. 25-29.
[3] Kostopoulos, G. (c2013). Cyberspace and cybersecurity. Boca Raton: CRC Press.
[4] Kumar, V., Chakraborty, S., Barbhuiya, F.A. & Nandi, S. (2012). Detection of stealth Man-in-the-Middle attack in wireless LAN. Proceedings of 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, PDGC 2012, pp. 290.
[5] Parkavi, D. & Seethalakshmi, R. (2014). Secure data transaction using cryptographic algorithm in ARM. International Journal of Applied Engineering Research, vol. 9, no. 16, pp. 3183-3194.
[6] Singer, P. (c2014). Cybersecurity and cyberwar: what everyone needs to know. Oxford: Oxford University Press.
[7] Vacca, J. (c2013). Computer and information security handbook. 2nd ed. Waltham, MA: Elsevier/Morgan Kaufmann.
[8] Vallivaara, V., Sailio, M. & Halunen, K. (2014). Detecting man-in-the-middle attacks on non-mobile systems. CODASPY 2014 - Proceedings of the 4th ACM Conference on Data and Application Security and Privacy, pp. 131.
[9] Wu, C. & Irwin, J. (c2013). Introduction to computer networks and cybersecurity. Boca Raton: CRC Press.
[10] Number of smartphone users* worldwide from 2014 to 2019 (in millions). 2014. The Statistics Portal. Available from: http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
[11] Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015. 2014. Gartner [online]. Barcelona. Available from: http://www.gartner.com/newsroom/id/2905717

David Malanik
Born in Zlin, Czech Republic, 1. March 1984. Master degree in Information technology 2008, Tomas Bata University in Zlin. Ph.D. Thesis based on the user identification provided by the neural network, 2011, Tomas Bata University in Zlin.
SENIOR LECTURER at Tomas Bata University in Zlin, Department of Informatics and Artificial Intelligence.
Main specialization: computer security, computer viruses, penetration testing, artificial neural network, computer networks.

Roman Jasek
Head of department of informatics and Artificial intelligence at the Faculty of Applied Informatics in Tomas Bata University in Zlin, Czech Republic. He deals with the security of information systems and security application on the mobile platform. The team, working under his direction, is deals with industrial applications using artificial intelligence.