INTERNATIONAL SCIENTIFIC CONFERENCE “ARCHIBALD REISS DAYS”
THEMATIC CONFERENCE PROCEEDINGS OF INTERNATIONAL SIGNIFICANCE

INTERNATIONAL SCIENTIFIC CONFERENCE

"ARCHIBALD REISS DAYS"

Belgrade, 2-3 October 2018

THEMATIC CONFERENCE PROCEEDINGS
OF INTERNATIONAL SIGNIFICANCE

VOLUME II

Academy of Criminalistic and Police Studies
Belgrade, 2018

Publisher
ACADEMY OF CRIMINALISTIC AND POLICE STUDIES
Belgrade, 196 Cara Dušana Street (Zemun)

Computer Design
JOVAN PAVLOVIĆ
DRAGOLJUB MILUTINOVIĆ

Impression
200 copies

Print
Službeni glasnik, Belgrade

THE CONFERENCE AND THE PUBLISHING OF PROCEEDINGS WERE SUPPORTED
BY THE MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGICAL
DEVELOPMENT OF THE REPUBLIC OF SERBIA

ISBN 978-86-7020-405-8
ISBN 978-86-7020-190-3

HONORARY COMMITTEE

Goran Bošković, PhD, Academy of Criminalistic and Police Studies, Belgrade, **President**
Sima Avramović, LLD, Dean of the Faculty of Law, Belgrade
Ivica Radović, PhD, Dean of the Faculty of Security, Belgrade
Major-General Mladen Vuruna, PhD, Rector of the University of Defence, Belgrade
Branislav Đorđević, PhD, Director of the Institute of International Politics and Economics, Belgrade

International members

Olivier Ribaux, PhD, Director of the School of Criminal Justice, University of Laussane, Switzerland
Norbert Leitner, PhD, President of the Association of European Police Colleges,
Director of SIAK, Vienna, Austria
General Cao Shiquan, PhD, President of the Chinese National Police University,
Beijing, People's Republic of China
Hao Hongkui, PhD, President of the Criminal Investigation Police University of China,
Shenyang, People's Republic of China
Major-General Andrey Kochin, PhD, Acting Head of the St. Petersburg University
of the Ministry of Internal Affairs of the Russian Federation
Major-General Vladimir Tretyakov, PhD, Chief of the Volgograd Academy
of the Ministry of Internal Affairs of the Russian Federation
Police Colonel Roman Blaguta, PhD, Rector of the Lviv State University of Internal Affairs, Ukraine
Major-general Vladimir Bachila, PhD, Head of the Academy of the Interior Ministry of the Republic of Belarus
José García Molina, PhD, Director of Spanish Police Academy, Ávila
Police Colonel Marek Fałdowski, PhD, Commandant-Rector of Police Academy, Szczytno, Poland
Lucia Kurilovská, PhD, Rector of the Academy of the Police Force, Bratislava, Slovakia
Major-General Panagiotis Kordolaimis, Commander of the Hellenic Police Academy, Athens, Greece
Yilmaz Çolak, PhD, President of the Turkish National Police Academy, Ankara
Adrian Iacob, PhD, Rector of the Police Academy "Alexandru Ioan Cuza", Bucharest, Romania
Simion Carp, PhD, Rector of the Academy "Ştefan cel Mare",
Ministry of the Interior of the Republic of Moldova, Kishinev
Zoltán Rajnai, PhD, Dean of the Donát Bánki Faculty of Mechanical and Safety Engineering,
Óbuda University, Hungary
Andrej Sotlar, PhD, Dean of the Faculty of Criminal Justice and Security, Ljubljana, Slovenia
Nikola Dujovski, PhD, Dean of Faculty of Security, Skopje, Macedonia
Predrag Ćeranić, PhD, Dean of the Faculty of Security Science, University of Banja Luka, BiH
Nedžad Korajlić, PhD, Dean of the Faculty for Criminal Justice, Criminology and Security Studies,
University of Sarajevo, BiH
Velimir Rakočević, PhD, Dean of the Faculty of Law, Podgorica, Montenegro
Boban Šaranović, Director of Police Academy, Danilovgrad, Montenegro

PROGRAMME COMMITTEE

Biljana Simeunović-Patić, PhD, UCIPS, Belgrade, **President**
Aleksey Bashan, PhD, Academy of MoI of Belarus
Andy Bécue, PhD, University of Lausanne, Switzerland
Jay Dawes, PhD, University of Colorado, Colorado Springs, USA
Gorazd Meško, PhD, Faculty of Criminal Justice and Security, Ljubljana,
University of Maribor, Slovenia
Jozef Meteňko, PhD, Academy of Police Force, Bratislava, Slovakia
Imre Rudas, PhD, Obuda University, Budapest, Hungary
Slobodan Simonović, PhD, Western University, London, Canada
David D. Stephens, M.S., Forensic Science Consultants, Inc., USA
John Winterdyk, PhD, Mount Royal University, Calgary, Canada
Đorđe Đorđević, PhD, UCIPS, Belgrade
Zoran Đurđević, PhD, UCIPS, Belgrade
Stevo Jaćimovski, PhD, UCIPS, Belgrade
Saša Mijalković, PhD, UCIPS, Belgrade
Dragan Mlađan, PhD, UCIPS, Belgrade
Obrad Stevanović, PhD, UCIPS, Belgrade
Dane Subošić, PhD, UCIPS, Belgrade
Slaviša Vuković, PhD, UCIPS, Belgrade
Petar Čisar, PhD, UCIPS, Belgrade
Smilja Teodorović, PhD, UCIPS, Belgrade
Jelena Radović-Stojanović, PhD, UCIPS, Belgrade
Dragoslava Mićović, PhD, UCIPS, Belgrade

ORGANIZING COMMITTEE

Darko Simović, PhD, UCIPS, Belgrade, **President**
Saša Milojević, PhD, UCIPS, Belgrade
Aleksandar Bošković, PhD, UCIPS, Belgrade
Valentina Baić, PhD, UCIPS, Belgrade
Nenad Koropanovski, PhD, UCIPS, Belgrade
Aleksandra Ljuština, PhD, UCIPS, Belgrade
Nikola Milašinović, PhD, UCIPS, Belgrade
Brankica Popović, PhD, UCIPS, Belgrade

TABLE OF CONTENTS

TOPIC III
Police organization – structure,
Functioning and human resources

OVERVIEW OF SOME SECURITY ASPECTSOF SMART PHONES

Petar Čisar, PhD
University of Criminal Investigation and Police Studies, Belgrade
petar.cisar@kpa.edu.rs
Imre Rudas, PhD
Obuda University, Hungary
rudas@uni-obuda.hu

Abstract: Smart phones or mobile phones with advanced capabilities are used by more people. Their popularity and relatively weaker security level have made them attractive targets for attackers. Mobile phone security in the beginning has not kept pace with traditional computer security. Security methods, such as firewalls, antivirus software and encryption, were insufficiently represented on mobile phones, and mobile operating systems were not updated as frequently as those on personal computers. However, mobile security nowadays is a rapidly growing field in the security area. With the increase in the number of mobile devices and their applications, the need for mobile security has increased extremely over the past several years. This paper gives an overview of some of the security aspects that must be considered when choosing a particular model of a smart phone with a satisfactory level of security: biometrics, encryption, hardware-assisted security, sandboxed user data, VPN possibility etc. A special accent in the paper is placed on newer types of processors as one of the most important components of the mobile device and their security possibilities. A comparative analysis of the key technical characteristics of the most commonly used newer processors is also given. In addition, the paper also focuses on the use of mobile security software and Android browsers, pointing out its numerous useful features.

Keywords: smart phones, security, processor, metrics, mobile security software, Android browser

INTRODUCTION

Smart phones are becoming more popular and numerous users decide to buy a smart phone for their mobile communication. They offer more features than classic mobile phones, and one of the reasons of their popularity is the ability to expand device capabilities by adding new applications. Smart phones have been present in the mobile phone market for a long time, but they have gained real popularity with the appearance of iPhone smart phone (Apple) and Android operating system (Google).

Android and iOS are the two most widely used operating systems (OS) for smart mobile terminal devices. Although these two OSs share some similarities, such as layered architecture, the most important difference is in the type of code. Android is an open source operating

system, while iOS is a closed code. Closed nature makes the iOS operating system less flexible but less vulnerable.

Every advanced mobile phone, as PCs, is a potential target of attacks. These attacks use vulnerability characteristics for smart phones that can originate from their communication mode - for example, GSM, short message service (SMS), multimedia messaging service (MMS), Wi-Fi and Bluetooth, the worldwide accepted standards for mobile communications. There are additionally misuses which are focused on software weaknesses in the web browser or operating system. Besides, a few attack types depend on hardware vulnerabilities (electromagnetic waveforms, juice jacking, jail-breaking and rooting).

In accordance with the above, in general terms, three models of mobile platform threats can be formulated:

Attack with physical access - try to unlock phone, exploit vulnerabilities to bypass locking

System attacks - exploit vulnerabilities in mobile platform using web downloads, malformed data, operating systems etc.

Application attacks - use malicious application to steal data, misuse system and hijack other applications.

Android is considered to be one of the most common mobile operating systems. Its general security vulnerabilities can be formulated as: open source nature, fragmentation, slow moving upgrades, JavaScript binding over HTTP vulnerability and third party applications stores.

In the following figure, the degree of threat from malicious mobile malware is illustrated and it represents the number of detected malware packages worldwide.

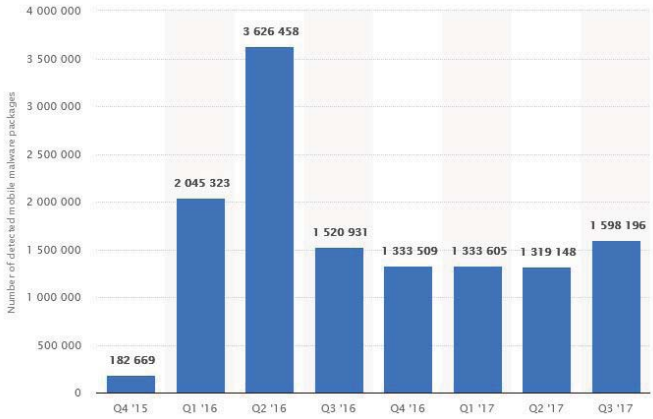

Figure 1. *Number of Detected Malicious Installation Packages on Mobile DevicesWorldwide (from 4th quarter 2015 to 3rd quarter 2017)*[1]

There are various organizations worldwide focused on improving the mobile security. One of them is Open Web Application Security Project (OWASP). This is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs (*application programming interface)* that can be trusted. The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The OWASP Mobile Security Project is a centralized resource intended to give developers

1 Statista, The Statistics Portal, https://www.statista.com/statistics/653680/volume-of-detected-mobile-malware-packages/

and security teams the resources they need to build and maintain secure mobile applications. Through the project, the goal is to classify mobile security risks and provide developmental controls to reduce their impact or likelihood of exploitation.

The OWASP identified and categorized the following top ten mobile risks in 2016:[2]

Improper Platform Usage (M1) – Misuses of a platform feature or failure to use platform security controls is covered in this category. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is a part of the mobile operating system. There are several ways that mobile apps can experience this risk.

Insecure Data Usage (M2) - This new category is a combination of M2 + M4 from Mobile Top Ten 2014. Insecure data storage and unintended data leakage are covered.

Insecure Communication (M3) - Poor handshaking, incorrect SSL versions, weak negotiation, clear text communication of sensitive assets are covered.

Insecure Authentication (M4) - Notions of authenticating the end user or bad session management is captured in this category. This can include:

- Failing to identify the user at all when that should be required
- Failure to maintain the user's identity when it is required
- Weaknesses in session management

Insufficient Cryptography (M5) - The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Failing to use cryptography at all, when it should, probably belongs to M2. M5 is for issues where cryptography was attempted but it wasn't done correctly.

Insecure Authorization (M6) - Any failures in authorization are to be captured in this category (authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (device enrolment, user identification, etc.).

However, an authentication failure appears if the application does not authenticate users at all in a situation where it should. In this case, it is not considered an authorization failure.

Client Code Quality (M7) - This was the "Security Decisions Via Untrusted Inputs", one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.

Code Tampering (M8) – Binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification are covered in this category.

Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.

Reverse Engineering (M9) – Analysis of the final core binary to determine its source code, libraries, algorithms, and other assets is included in this category. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.

2 https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Extraneous Functionality (M10) - Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.

SECURITY AND PRIVACY ASPECTS OF SMART PHONES

Android, as one of the most popular operating systems for smart phones (mobile phones with advanced capabilities) today, due to its openness of code, carries with it a series of potential security problems, which can be formulated in several categories (Čisar, 2017):

Open source - Since the entire source code is easily accessible, people with malicious intent may seek the ability to create security issues.

Fragmentation - With hundreds of manufacturers, who all contribute to the development of the operating system, viruses and malware of new generations easily exploit the weaknesses that are not found in Stock Android.

Slow moving upgrades - Android users are known for delays in adopting new patches and versions or migrating to a new version of the operating system. Using an outdated version of the operating system becomes more and more vulnerable to data and identity theft.

JavaScript binding over HTTP - Programmers can accept JavaScript connection method as the easiest way to load web content in an Android application, but this can be a source of major security problems. By opening the web view with HTTP, it gives the possibility for attackers to completely remove HTTP data or events by remote execution of application codes.

Third party Application Stores - Although this does not have to be a security problem in direct connection with Android, it deserves a certain amount of attention. The fact is that these stores contain more hidden malware than in the Google Play Store. Although not all third-party application stores are risky, it's still necessary to look carefully at those in which the application will be installed (available). The installed application in these stores does not necessarily have security threats, but it can create a bad reputation if users for some reason are dissatisfied with them.

When we talk about security and privacy aspects of smart phones, there are several differentiating factors which have to be identified:[3]

- Biometrics: There are two security directions including fingerprint scanners and other biometric unlocking algorithms. To begin with, there is a possibility that if someone's biometric identifiers were stolen, he wouldn't be able to simply change them as a password, making them for all time potential security risk. The second direction of reasoning is that if a security approach is less demanding, they'll probably really utilize it, in which case biometrics are better for general security. It depends on the user whether the fingerprint sensor is acceptable to him or not, but it is important to emphasize that having such option empowers other security-related features (for example, LastPass' fingerprint login).

- Encryption: There are two types of encryptions: file-based encryption (FBE) and full disc encryption. One of the two types is used by the majority of modern phones. FBE allows single files to be locked with different keys and it makes it more effective than full disc encryption since it uses only one key to lock the whole disc partition**.** Phones use the AES encryption standard, with 128/256-bit keys to decrypt the data.

3 Gadget Hacks, https://smartphones.gadgethacks.com/how-to/4-best-phones-for-privacy-security-0176106/

• Hardware-Assisted Security: Each phone calls upon the hardware to improve the general security of the device. iOS devices use the hardware to assist with encryption whereas the Android devices utilize the hardware to store cryptographic keys.

• Sandboxed User Data: If privacy is one among high issues, a user will need to keep up separate areas on their phone — perhaps one for work, and another for personal usage. If so, it is important that the data from every user account is completely separated ("sandboxed") and that the Android phones support this feature.

• Limit Advertisement (Ad) Tracking: Phones that work with Apple and Google services preinstalled, use an advertising tracking identifier (ID) to help marketing partners send targeted ads. This ID follows the user who uses different applications and services, which is problematic from the aspect of privacy. Apple allows restrict applications' abilities to view and use this identifier, while Google merely lets a user reset the ID and opt out of seeing personalized ads on Android devices.

• VPN Possibility: A virtual private network (VPN) allows rerouting internet traffic through an external server. Encrypt data traffic for obtaining increased level of security can be provided to a user by a VPN service. With Android devices, user can direct all types of internet traffic through a VPN. With an iPhone, a user can only use a VPN over Wi-Fi, unless they are willing to reset his device and enable "Supervised Mode" to get the VPN working on his mobile data connection.

• Block Internet Access for Applications: If someone does not want applications "phoning home," the ability to block internet access on a per-app basis is a significant advantage. With Android, this can be done by setting up a local VPN. With iOS, a user can easily disable mobile data access for an app, however, it is not possible to restrict Wi-Fi connectivity.

• Data Wipe After Failed Login: Some phones have a feature that triggers an automatic factory reset when someone attempts to enter user's PIN or password too many times, if enabled. This is very effective when it comes to fending off intruders, as it makes brute-force password attacks impossible.

• Password Management Service: The password management service (LastPass) has varying degrees of functionality on different phones. Some of the devices allow user to log into the service using his fingerprint, others will auto-populate passwords into applications and websites for the user.

• Provide Security Center Application: If someone considers the security very important, it is recommended to have a centralized application that helps handling security needs. For example, the DTEK security platform (by BlackBerry) gives user an overview of his phone's actual security level and allows him to easily adjust important security settings.

• Operating System Common Vulnerabilities and Exposures (CVE): The majority of modern phones run either iOS or Android. In recent years, both of these operating systems have had numerous CVEs discovered, so it is important to keep track of exactly how vulnerable they are.

• Security Patch Timeframe: Apple doesn't adhere to a specific timeframe with its security patches. However, updates are generally issued within a month of security bugs being discovered. Android releases security patches monthly and leaves it to the original equipment manufacturer (OEM) to distribute to their devices. Since the Pixel 2 is a Google device, it will get Android security patches first.

• Bug Prize: Some device manufacturers offer a prize for anyone who can find significant weaknesses in their phone's software, stimulating the process of discovering and closing security loopholes (bugs). With a higher bounty, people will generally be more motivated

to find these bugs. Some companies invite only trusted bug reporters to earn a bounty while others will let anybody report bugs and claim the bounty.

Hardware Factors				
Biometrics	Fingerprint Scanner	Facial Recognition	Fingerprint Scanner	Fingerprint Scanner
Encryption	Full Disk (AES 128)	File-Based (AES 256)	File-Based (AES 256)	File-Based (AES 256)
Hardware Assisted Security	Hardware Stored Encrypted Keys	Dedicated Hardware Chip	Hardware Stored Encrypted Keys	Hardware Security Module
OS Considerations				
Sandboxed User Accounts	Yes	No	Yes	Yes
Restrict Ad Tracking	No	Yes	No	No
Always-On VPN	Yes	Supervised Mode Only	Yes	Yes
Block Internet Access for Apps	With VPN App	Mobile Data Only	With VPN App	With VPN App
Data Wipe After Failed Login	Yes	Yes	No	No
Important Apps				
LastPass Fingerprint Login	Yes	No	Yes	Yes
LastPass Auto-Populate	Yes	No	Yes	Yes
Stock Security Center App	DTEK	None	Knox	None
Field Testing				
OS CVEs (3-Year Total)	1383	913	1383	1383
Security Patch Time Frame	1 Month	Within 1 Month	1 Month	1 Month
Bug Bounties	Open (Undisclosed)	Closed (Up to $200K)	Open (Up to $200K)	Open (Up to $200K)

Figure 2. *Different Metrics for Ensuring Security and Privacy (BlackBerry KEYone (1st column), iPhone X (2nd column), Samsung Galaxy Note 8 (3rd column), Google Pixel (4th column))*[4]

PROCESSORS

The processor is the main part of a smartphone, which has a dominant influence on the operating speed. Therefore, it is crucial that it operate at a higher speed. The clock rate and the number of cores are not the only factors. They are called system-on-a-chip (SoC). In general, a SoC consists of a central processing unit (CPU), graphics processing unit (GPU), modem, multimedia processor, security device and signal processor.[5]

Qualcomm's Snapdragon 845 system-on-chip is the latest generation processor. Besides being powerful, energy-efficient, and optimized for artificial intelligence (AI), it is also highly secure. The Snapdragon 845 is the first to feature Qualcomm's secure processing unit (SPU), a new subsystem designed to protect biometrics, data, payment information, and SIM data. When someone performs some kind of action (save a file or take a photograph), the system-

4 Gadget Hacks, https://smartphones.gadgethacks.com/how-to/4-best-phones-for-privacy-security-0176106/
5 AndroidPIT, https://www.androidpit.com/fastest-smartphone-processors

on-chip's SPU will generate a unique key. In addition, applications (for instance, WeChat and Facebook) can use the SPU to generate keys as needed.[6]

The SPU is completely isolated from the system. Although it is not a "system master," meaning it cannot access information from other systems or take control of new processes, it is able to access information from other systems independently.

It plays a crucial role in biometrics. In future, the manufacturer wants to store biometric data inside the SPU, run any necessary authenticator code inside the SPU, and terminate the data within the SPU itself. This chip is presented as a safer alternative to secure elements like ARM's TrustZone, which have been exploited before.

Table 1. *Newer SoCs comparison7*

	Snapdragon 845 (Q1 2018)	Snapdragon 835 (Q2 2017)	Apple A11 Bionic (Q3 2017)	Kirin 970 (Q3 2017)
CPU (Central Processing Unit) Architecture	64-bit	64-bit	64-bit	64-bit
CPU Cores	Octa Core 4 x 2.8 GHz Kryo 385 4 x 1.7 GHz Kryo 385 X20 LTE modem	Octa Core CPU 4 x 2.45 GHz Kryo 280 4 x 1.9 GHz Kryo 280 X16 LTE modem	Hexa-core (2 Ч Monsoon + 4 Ч Mistral) Max up to 2.34 GHz	4 x Cortex A73 at 2.4 GHz 4 x Cortex A53 at 1.8 GHz
GPU (Graphics Processing Unit)	Adreno 630	Adreno 540	Apple designed custom 3 core(s) GPU	Mali G72 MP12 12-core
RAM	Up to 8 GB dual channel LPDDR4x	Up to 8 GB dual channel LPDDR4x	3 GB of LPDDR4	Up to 8 GB dual-channel LPDDR4
Manufacturing Technology	10 nm FinFET	10 nm FinFET	10 nm FinFET	10 nm FinFET
NPU (Neural Processing Unit)	Hexagon DSP 2nd generation	Hexagon DSP	Neural Engine	NPU
LTE (Long Term Evolution)	Cat 18, up to 1.2 Gbps	Cat 16, up to 1 Gbps	Cat 16, up to 1 Gbps	Cat 18, up to 1.2 Gbps

Popularity of CPU's in modern phone models:

- BlackBerry KEYone - Qualcomm Snapdragon 660
- iPhone X - Apple A11, Kirin 970
- Samsung Galaxy S8 Note - Qualcomm Snapdragon 835
- Google Pixel 2 - Qualcomm Snapdragon 835

6 Xda-developers, https://www.xda-developers.com/qualcomm-snapdragon-845-secure-processing-unit/

7 SuggestPhone, https://www.suggestphone.com/blog/snapdragon-835-vs-845-apple-a11-bionic-comparison

- Huawei Mate 10 Pro - Kirin 970
- HTC U11 - Qualcomm Snapdragon 835
- Sony Xperia XZ Premium - Qualcomm Snapdragon 835
- LG V30 - Qualcomm Snapdragon 835
- OnePlus 5T - Qualcomm Snapdragon 835

CPU SECURITY

Snapdragon 845:[8] Includes a hardware isolated subsystem called the Secure Processing Unit (SPU). The SPU is an isolated security-focused processor embedded in the system-on-a-chip. The manufacturer wants to store all that biometric data in the vault-like environment, which is similar to what Apple does on its A11 Fusion processor in the iPhone. The Secure Enclave Processor has its own microprocessor and encrypted memory and it handles ultra-sensitive data like Face ID data and decryption keys. The SPU stores similar sensitive data (payment information, SIM information and more) and it is kept separate from other components to prevent hacking.

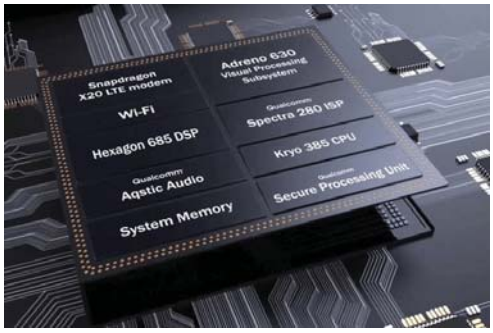

Figure 3. *Snapdragon 845 Structure*

Snapdragon 835:[9] Built upon the strength of the Snapdragon security platform, this chip is designed to safeguard the entire device from mobile security threats. The mobile security framework is engineered to provide multilevel security by combining a hardware-level solution with next-generation software for robust biometrics security. The newest security components include a secure camera, secure token and Smart Protect for latest mobile security measures.

MOBILE SECURITY SOFTWARE

This type of software will improve mobile device's performance by cleaning junk files (analyze and safely remove the junk files that take up storage space), optimizing device memory (phone boost - kill off buggy applications that slow down the device and steal memory), providing antivirus and antimalware protection (keeping the device safe from viruses, trojans,

8 Digital Trends, https://www.digitaltrends.com/mobile/qualcomm-snapdragon-845-security/
9 Qualcomm, https://www.qualcomm.com/solutions/mobile-computing/features/security/mobile-security

vulnerabilities, spyware and protecting personal information) and managing the installed applications (battery saver - hibernate background battery draining applications to save power).

On-device protections (services) are: malicious applications (anti-malware protection and removal options for downloaded potentially harmful applications), safety net (protection from network and application-based threats), safe browsing (protection from deceptive websites - includes a web filtering feature to block dangerous sites), developer APIs (allows third-party applications to use security services), Android device manager (protection for lost or stolen devices – anti-theft), smart lock (encourage lock screen adoption by reducing friction around device unlock).

The aim of the research carried out by AV-Test (the independent IT-security institute) is to directly detect the latest malware, to analyze it by using state-of-the-art methods and to inform customers of the top-quality results obtained. All products tested and inspected by AV-Test undergo complex test procedures in terms of their performance in the following categories:[10]

- protection (protection against malicious Android applications)
  - detection of the latest Android malware in real-time
  - detection of the latest Android malware discovered in the last 4 weeks
- usability (impact of the security software on the usability of the device)
  - performance: the battery life is not impacted by the application
  - performance: the device is not slowed down by the application during normal usage
  - performance: too much traffic is not generated by the application
  - false warnings during installation and usage of legitimate applications from Google Play Store
  - false warnings during installation and usage of legitimate software from third party application stores
- features (further important security features)
  - Anti-Theft (Remote-Lock / Remote-Wipe / Locate): Locate, Lock or Wipe your device when it is lost or stolen
  - Call Blocker: Block calls from specific or unknown numbers
  - Message Filter: Filter messages and/or mails for unwanted content
  - Safe Browsing: Protection of malicious websites and/or against phishing
  - Parental Control: Features to control or observe the activity of children on the device
  - Backup: Personal data can be saved to SD-card or cloud storage
  - Encryption: Any kind of encryption is supported (e.g. device encryption, SD-card encryption or VPN)

The testing results for January 2018 are given by the figure below.

10 AV-Test, https://www.av-test.org/en/antivirus/mobile-devices/

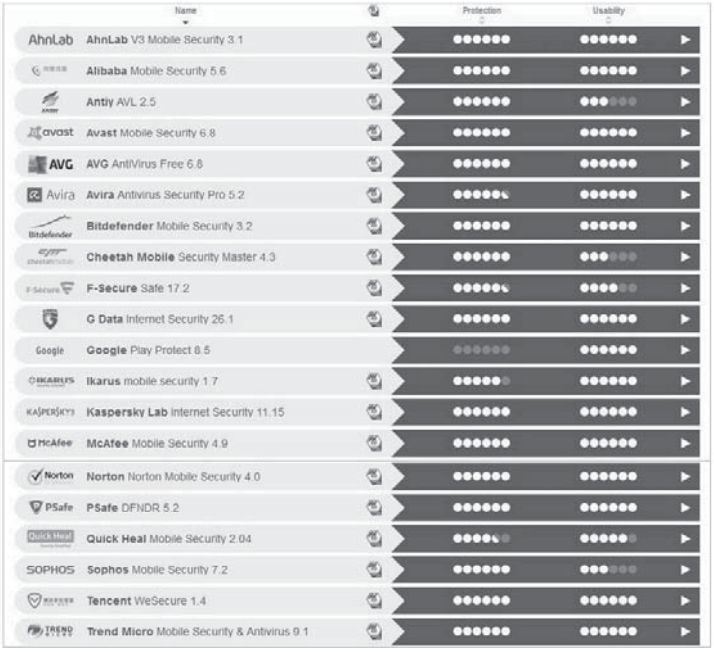

Figure 4. *AV-Test results for January 2018*

ANDROID BROWSERS

The choice of mobile phone's web browser affects the overall security of communication. There are several desirable security options to consider when choosing and installing an Android browser:

- Private (incognito) browsing: The ability to browse the web secretly, without data saving and syncing across devices. Browsing history and logins are not recorded while using this mode. History, cookies and site data are never stored on disk, and never transmitted.
- Advertisements blocker: The ability to blocks advertisements in web pages, either natively or with an extension.
- Tracking protection: Trackers are used by corporations to gather information (such as device information, time, and type of browser) about the user when visiting their website. This protection blocks these trackers, disabling features like JavaScript, DOM (Document Object Model) storage, and cookies that are used by websites to record this information.
- Extensions: The ability to add extra features to the browser by installing small programs which enhance browsing experiences.
- Password manager: The ability to store password information to autofill frequently visited websites. Privacy protection: Automatically clears all browsing history when the application closes.
- HTTPS everywhere: Enforces SSL (Secure Sockets Layer) security wherever that's possible (encrypts communications with many major websites, making browsing more secure).

• Fraud prevention: Warns the user when browsing potentially fraudulent or malicious websites.

• Malicious download protection: Scans apk-file downloads for malware, keeping a device secure.

CONCLUSION

Based on the various aspects of security shown in the paper, it can be concluded that ensuring a sufficiently high level of security for mobile phones is a complex task. Namely, it is necessary to provide the implementation of a wide range of system, hardware and application security methods. In that sense, it is recommended to use mobile devices with newer generation processors, which incorporate numerous improvements from the security domain. Also, the application of adequate and up-to-date mobile security software can significantly raise the level of security.

LITERATURE

1. Alqahtani AS (2013). Security of Mobile Phones and their Usage in Business, International Journal of Advanced Computer Science and Applications, Vol. 4, No. 11
2. Androulidakis I (2016). Mobile Phone Security and Forensics: A Practical Approach, Springer
3. Au MH & Choo R (2016). Mobile Security and Privacy: Advances, Challenges and Future Research Directions, 1st Edition, Syngress
4. Bergman N, Stanfield M, Rouse J & Scramblay J (2013). Hacking Exposed Mobile: Security Secrets & Solutions, 1st Edition, McGraw-Hill Education
5. Čisar P (2017). General Aspects of Application IT Security, NBP - Journal of Criminalistic and Law, Academy of Criminalistic and Police Studies, No. 2, Belgrade, pp. 33-46.
6. Doherty J (2015). Wireless and Mobile Device Security, Jones & Bartlett Learning, 1 edition
7. La Polla M, Martinelli F, Sgandurra D (2012). A Survey on Security for Mobile Devices, IEEE Communications Surveys & Tutorials, http://www.iit.cnr.it/sites/default/files/A survey on Security for mobile devices.pdf
8. Mobile Technologies Security (2011). The Government of the Hong Kong Special Administrative Region, https://www.infosec.gov.hk/english/technical/files/mobilets.pdf
9. Urbas G & Krone T (2006). Mobile and wireless technologies: security and risk factors, Trends & Issues in Crime and Criminal Justice, No. 329, Australian Institute of Criminology
10. AV-Test, https://www.av-test.org
11. ESET, ESET Mobile Security, 2011, http: //www.eset.com/us/home/products/mobile-security/security/Mobile brochure MWC2015.pdf
12. Kaspersky Lab, Kaspersky Security for Mobile, 2015, https://media.kaspersky.com/en/business-security/Mobile brochure MWC2015.pdf
13. Qualcomm, https://www.qualcomm.com