A Risk Assessment Method for Smartphones

Marianthi Theoharidou, Alexios Mylonas, Dimitris Gritzalis

A Risk Assessment Method for Smartphones

Marianthi Theoharidou[1], Alexios Mylonas[1,*] and Dimitris Gritzalis[1]

[1] Information Security and Critical Infrastructure Protection Research Laboratory
Dept. of Informatics, Athens University of Economics and Business (AUEB)
76 Patission Ave., Athens, GR-10434 Greece
{mtheohar,amylonas,dgrit}@aueb.gr

Abstract. Smartphones are multi-purpose ubiquitous devices, which face both, smartphone-specific and typical security threats. This paper describes a method for risk assessment that is tailored for smartphones. The method does not treat this kind of device as a single entity. Instead, it identifies smartphone assets and provides a detailed list of specific applicable threats. For threats that use application permissions as the attack vector, risk triplets are facilitated. The triplets associate assets to threats and permission combinations. Then, risk is assessed as a combination of asset impact and threat likelihood. The method utilizes user input, with respect to impact valuation, coupled with statistics for threat likelihood calculation. Finally, the paper provides a case study, which demonstrates the risk assessment method in the Android platform.

Keywords: Smartphone, Risk Assessment, Android, Security, Threat.

1 Introduction

Smartphones' popularity lies mainly with their pervasiveness, which stems from their small size, advanced processing and connectivity capabilities, reduced cost, and their ability to host multi-purpose third party applications. Smartphones host heterogeneous data such as multimedia, sensor data, communication logs, data created or consumed by applications, etc. A smartphone user carries the device on multiple locations throughout the day, and allows connections to various networks that are often not secure. As the same device may be used for both, work and leisure purposes, smartphones often contain a combination of valuable personal and business data.

The complexity of administrator attempts to secure organisation assets rises, as users continue to bring their own smartphones in corporate premises [17]. Often, organizations are not prepared to manage smartphone heterogeneity, especially when the required resources or expertise is not present (consumerization). Smartphones extend the business perimeter, while existing security and privacy perimeter-oriented mechanisms are inadequate [18]. In this context, the importance of smartphone data, in conjunction with their ability to interact with corporate assets, make them economically attractive to attackers [2]. Hence, traditional risks (e.g. theft, fraud, etc.) may reappear with increased impact. They can pose a security challenge [4] or take place

adfa, p. 1, 2011.

using new attack vectors, e.g., using smartphone location capabilities for surveillance [16]. In addition, smartphones implement different security models, which make traditional countermeasures ineffective.

Traditional risk assessment methods treat smartphones as an asset of a business information system, similarly to a personal computer or a laptop. They treat the smartphone as a single entity, where threat and vulnerability assessment are performed on the asset as a whole. Although a smartphone can be viewed as a kind of small scale information system, making existing methods applicable, such an assessment is not ideal for risks that target device (sub)assets, e.g. GPS sensor (i.e. surveillance), logs (i.e. call logs disclosure), etc. This is due to the fact that they do not take account smartphone-specific threats, neither the unique vulnerabilities that a smartphone security model introduce. Furthermore, most risk assessment methods are not intended for users, but mainly for businesses. Thus, a targeted risk assessment method is useful, so as to assess user-specific parameters and smartphone-specific threats, in a considerably more fine-grained fashion. We contribute towards this direction by identifying smartphone assets and threats, as well as by proposing a risk assessment method specifically tailored for smartphones.

The paper is organized as follows. Section 2 provides the reader with a smartphone definition and smartphone data taxonomy. In Section 3 the proposed risk assessment method is introduced. The method is applied in Section 4, through the use of a case study. Method limitations and further research ideas are discussed in Section 5.

2 Smartphone: Definition and Assets

The term smartphone is frequently used by the industry and research community to refer to state-of-the-art cell phone devices. These devices are considered 'smart', and are distinguished from ordinary and technologically constrained cell phones. The latter, which are referred to as feature phones, are often restrained by small screen size, limited processing and network capabilities, and execute, in general, a proprietary and not adequately documented operating system. Thus, their security is mainly based on secrecy or as the IT security community refers to, as "security by obscurity".

In contrast with the term 'feature phone', a widely accepted definition for 'smartphone' can hardly be found in the literature. Becker et al. [1] define smartphones as devices which: (a) "contain a mobile network operator smartcard with a connection to a mobile network", i.e. a SIM or USIM card in GSM and UMTS systems, respectively, and, b) "have an operating system that can be extended with third-party software". However, this definition appears to be rather broad. Also, its properties are valid for feature phones. For instance, the Motorola V3i[1] feature phone would be incorrectly classified as a smartphone, as it contains a mobile carrier SIM card and has a proprietary OS that can be extended by third party applications (specifically with MIDP 2.0 Java applications).

The alternative definition of a smartphone, which is adopted here, is the following: smartphone is a cell phone[2] with advanced capabilities, which executes an identifi-

[1] http://www.motorola.com/mdirect/manuals/V3i_9504A48O.pdf

[2] A cell phone is a device which: a) is used primarily by its holder to access mobile network carrier services, e.g. phone calls, Short Message Services (SMS), etc., and b) contains a

able operating system allowing users to extend its functionality with third party applications that are available from an application repository. According to this definition, smartphones must include sophisticated hardware with: a) advanced processing capabilities (e.g. modern CPUs, sensors), b) multiple and fast connectivity capabilities (e.g. Wi-Fi, HSDPA), and (optionally) c) adequately limited screen sizes. Furthermore, their OS must be clearly identifiable, e.g. Android, Blackberry, Windows Phone, Apple's iOS, etc. Finally, the OS must allow third party application installation from application repositories ('app markets'), e.g. Android Market, BlackBerry App World, App Hub, App Store, etc.

2.1 Smartphone assets

A smartphone is viewed herein as a small-scale information system, which incorporates various assets. Jeon et al. [12] identify as its assets: (a) private information (address book, calling history, location information, etc.), (b) device (resources, i.e. CPU, RAM, battery), and (c) applications. Another report identifies six assets: (a) Personal data, (b) Corporate intellectual property, (c) Classified (governmental) information, (d) Financial assets, (e) Device and service availability and functionality, and (f) Personal and political reputation [6]. Another taxonomy includes Communication (Voice communication, Messaging), Data access (E-mail, Web access, Bluetooth/IR), Applications (Maps & Navigation, Social networking, etc.), and Device/Stored data (Physical device, Offline applications/Utilities, etc.) [14]. An assessment of security in the case of the Android platform [21] analyses: (a) private/confidential content stored on the device, (b) applications and services, (c) resources (battery, communication, RAM, CPU), and (d) hardware (device, memory cards, battery, camera).

Our analysis makes use of four asset types: a) Device, b) Connectivity, c) Data, and d) Applications. The Device asset type includes the physical device and its resources (e.g. battery, RAM, CPU etc.), but not the Data. The latter appear to be more complex and are analysed in the next section. Applications are viewed only as user services.

Smartphones use four Connectivity channels, namely: a). GSM services, i.e. messaging (SMS, EMS, etc.) and voice calls, b). PAN interface (e.g. Bluetooth, IrDA, etc.), a free and ad-hoc short-range data channel, c) WLANs (e.g. Wi-Fi, WiMAX, etc.), a fast data channel, and d) Cellular network, which provides Internet connectivity at variable speeds, depending on the carrier technology (e.g. GPRS, HSDPA, etc.).

2.2 Data Taxonomy

Data are classified on the basis of two dimensions, i.e., information type and source. Table 1 associates the two dimensions. These associations will be used later as the basis for the data impact valuation.

---

smartcard, which is controlled by the network carrier (i.e. SIM or USIM card) and incorporates a billing mechanism for the used network carrier services.

Table 1. Smartphone data taxonomy

Information Type / Source	Personal	Business	Government	Financial	Authenti-cation	Connecti-on/Service
Messaging	✓	✓	✓	✓	✓	
Device	✓	✓	✓	✓	✓	✓
USIM Card	some	some	some	some	✓	✓
Application	✓	✓	✓	✓	✓	✓
Use history & caching	✓	some	some	some		✓
Sensor	✓	✓	✓			
Input methods	✓	✓	✓	✓	✓	

Smartphone data hold various meanings. Their classification, according to the information type they may infer, led us to the following taxonomy:

Personal data are directly related to an identified individual. They are considered private and should not be made public. Examples include the content of a user's communication, images, videos, etc. Disclosure or unauthorized modification may result in embarrassment, reduction in self-esteem, or legal action.

Business data (or corporate intellectual property) refer to data with commercial and economic corporate significance. These include marketing information, products under design, etc. Unintended disclosure of this data to the public or competitors may lead to strategic advantage loss, copyright breach, loss of goodwill, etc. Such data are usually likely to exist in a 'personal' smartphone, if it is (even occasionally) used for business purposes.

Government data affect: (a) public order, (b) international relations, or (c) performance of public service organization(s). They differ from business data, because they hold national or international significance, as opposed to business value.

Financial data refer to records of financial transactions, current financial holdings or position. Unauthorized modification, disclosure, or unavailability may lead to financial loss or contract breach (e.g., due to delays).

Authentication data refer to user credentials, e.g. passwords, PINs, biometrics, etc. Their unauthorized access may lead to impact, such as financial loss, personal information disclosure, legal consequences, etc.

Connection/ Service data refer to data, which are required for network connections. They include connection identifiers, such as Wi-Fi MACs, IMSI, or IMEI, as well as data regarding the connection itself, such as the Wi-Fi joined networks history.

During regular (e.g., daily) use, data are used or stored on various sources. The following taxonomy is based on another dimension, i.e., data source [15]:

Messaging Data derive from: (a). mobile carrier messaging services i.e. Short Message Service (SMS), Enhanced Messaging Service (EMS), Multimedia Messaging Service (MMS), or (b). Instant and e-mail messages. They also include messaging logs, e.g. receiver, sender, delivery time and date, attachments, etc.
Device Data are data that (a) are not related to any third party application, or (b) contain device and OS specific information. They may reside in internal (e.g. flash drive, flash memory) and removable (e.g. microSD cards) storage media. Some examples include images, contact list, Wi-Fi MAC address, device serial number, etc.
(U)SIM Card Data reside either in a Universal Subscriber Identity Module (USIM) or Subscriber Identity Module (SIM) card. Typical examples are the International Mobile Subscriber Identity (IMSI)[3] and the Mobile Subscriber Identification Number (MSIN)[4]. This source often contains SMS and contact list entries.
Application Data include permanent or temporal data that are necessary for application execution. They may be stored as individual files, or constitute a local database, e.g. SQLite. A typical example is a flat dictionary text file.
Usage History Data are used for logging purposes, such as: (a) call history, which contains incoming or outgoing phone call logs, (b) browsing history, i.e. temporary data created while the user browses local or remote files, (c) network history logs for wireless connections, e.g. Wi-Fi SSIDS, Bluetooth pairing, and (d) event logs, which are created by the OS for system monitoring and debugging.
Sensor Data are created by dedicated hardware. Camera(s) and microphone(s) are two popular sensors. Other sensor hardware include: a) GPS sensor, b) accelerometer, c) gyroscope, d) magnetometer (i.e. digital compass), and e) proximity sensor. These are used to infer the exact device location, its orientation, the way the device is being moved, its heading direction, and the device distance from a surface, respectively. Sensor hardware, such as the light sensor and the temperature or pressure sensor, are present in some smartphones, measuring the device environment surroundings (context). Sensor data are mostly consumed on the fly and are not typically stored for later retrieval. Finally, they may be used as metadata (e.g. in geotagging where GPS data are embedded in photographs and videos).
User Input Data include user gestures, hardware button presses, and keystrokes from a virtual or smartphone keyboard. All involve user interaction with the device. User input data are often consumed on the fly, or stored in a keyboard cache for performance reasons (e.g. improvement of spelling software).

3 Smartphone Risk Assessment

To assess smartphone risk, one should first assess the impact of its assets. Then, assets should be related to smartphone threat scenarios. Impact assessment for each asset is described in the sequel.

[3] A unique number that identifies the subscriber to the network.
[4] The 10-digit phone subscriber number.

3.1 Asset impact

A key concept is, first, to involve the user with the initial impact valuation process. Then, the risk analyst should perform transparent associations and aggregations to calculate the overall risk.

Device. In typical risk assessment methods, physical assets are valued in terms of replacement or reconstruction costs, in a quantitative way. For a smartphone this refers to replacement or repair device cost, in the case of loss, theft, or damage. However, a smartphone contains, also, various information types, which need to be co-assessed in terms of impact.

Data. For information assets, a loss of confidentiality, integrity, or availability may be valued via several criteria [10], [14], i.e. personal information disclosure, legislation violation, contractual breach, commercial and economic interests, financial loss, public order, international relations, business policy and operations, loss of goodwill/reputation, personal safety, annoyance, etc. Due to the smartphone's multi-purpose nature, these impact types vary from purely personal ones, e.g. user annoyance, to typical information systems ones, e.g. commercial interests. This heterogeneity affects risk assessment. Adequate input from user is, thus, required, as clearly opposed to generic smartphone risk assessment [6], [21], which uses expert opinion.

In a 'personalized' (or 'itemized') risk assessment, the user is asked questions aiming to determine the existing data types (e.g., "Do you store personal data in your smartphone?", "Do you use your smartphone for business purposes? If so, do you work for a governmental institution?", or "Do you use your smartphone for financial transactions?", etc.).

In turn, for each identified data type, the user is invited to assess the impact of the following scenarios: "Which are the worst consequences if your <data type> are unavailable?", "Which are the worst consequences if your <data type> are disclosed to the public?" and "Which are the worst consequences if your <data type> are modified or damaged (deliberately/accidentally)?". The answers lead to impact calculation for each data type, namely the unavailability impact $\text{Impact}_{\text{UA}}$(data_type), the disclosure impact $\text{Impact}_{\text{DS}}$(data_type), and the modification impact $\text{Impact}_{\text{MD}}$(data_type).

Our approach adopts the "worst-case scenario" principle, i.e. the max operator is used to calculate the total scenario impact. The answers must follow a qualitative assessment of the impact types mentioned above, evaluated by the user with a 5-item[5] Likert scale (very low, low, medium, high, very high). For each impact criterion, a table needs to be produced, mapping each qualitative assessment to a comprehensive description. For example, for the 'personal information disclosure' criterion, the "very low" valuation may refer to "minor distress to an individual", as opposed to the "very high" one, which may refer to "significant distress to a group of individuals or legal and regulatory breach". Again, a map to quantitative values is required, because impact criteria cannot be considered equivalent. For instance, the "very high" valuation on 'personal information disclosure' must not be quantitatively valued equally to the "very high" valuation on 'personal safety'.

Connectivity. Likewise, the user assesses the network services impact: "Which are the consequences if you cannot use the SMS service?", "Which are the consequences if you cannot connect to a Wi-Fi network?", "Which are the consequences if

[5] Any number of levels between 3 and 10 can be used [10].

your Wi-Fi connection is been monitored?", etc. The assessment should follow the same valuation tables and scales, as the data valuation ones do. The resulting valuations, i.e. $Impact_{UA}$(channel), $Impact_{DS}$(channel), $Impact_{MD}$(channel), are used for risk assessment of threat scenarios which affect connectivity.

Applications. The same procedure can be used for user applications. Although this approach allows for a fine-grained impact valuation, it adds considerable complexity, as the applications may be numerous. It, also, assumes that a user has a clear perception of an application's significance, e.g. by using the application for some time. A trade-off could be the valuation of applications that the user identifies as more important. The assessment per application should follow the same valuation tables.

Total impact valuation. Based on the above, the user has assessed the impact of various scenarios (loss of availability, confidentiality and integrity) for all four smartphone asset types. These values are combined and used to assess the risk of the threats scenarios. For instance, the data type impact values are inferred to their associated data sources (see Table 1). This means that if a user has identified 'personal' and 'financial' data types on her smartphone, then the disclosure impact for the data source *'Messaging'* can be calculated, as follows:

$$Impact_{DS}(\text{Messaging}) = \max\{Impact_{DS}(\text{personal data}), Impact_{DS}(\text{financial data})\}$$

Likewise, the overall smartphone impact is the max impact from all four assets, i.e., the device, data, applications, and connectivity.

3.2 Threat

Threat likelihood is assessed on the basis of: (a) experience and applicable statistics, (b) vulnerabilities, and (c) existing controls and how effectively they may reduce vulnerabilities [10]. In this section a smartphone threat list is presented, together with a discussion on how threat likelihood may be assessed.

Table 2 presents a threat list expanding similar lists that are available in the smartphone literature [1], [5-6], [11-12], [14], [19], [21]. Each threat is grouped in the appropriate attack vector dimension (i.e. an asset utilization may be misused to impair another one (e.g. application access rights may be misused to leak private data)). Each threat is associated with the security attribute that it impairs.

A particular application may be an asset that needs protection and, at the same time, an attack access vector to other assets. For instance, the availability of a social networking application may be considered as a significant asset by a user (high impact), while being the attack vector for privacy threats. Even if this application is benign (i.e. not leaking any private data for malicious purposes), its privilege to access private data may be misused by a malicious application performing a deputy attack [3], [7], [9]. Though, it might be the case that a malicious application masquerades as a benign application (e.g. game) luring users into downloading it and, thus, being the attack vector themselves. Thus, such a smartphone privilege is herein considered vulnerability.

The permission acceptance likelihood differs in smartphone platforms. It depends on authorization decisions, as delegated by the platform security model. These decisions differ significantly [16] from allowing users to make security-critical authorization decisions (e.g. Android's community driven security model), up to placing functionality control barriers in applications that enter application repository (e.g. the 'walled garden' approach of Apple's App Store).

Table 2. Smartphone threats

Dimension	Threat	C	I	A
Network Connectivity	T1 Spoofing	✓	✓	✓
	T2 Scanning	✓		
	T3 Denial of Service, Network congestion			✓
	T4 Spam, Advertisements			✓
	T5 Eavesdropping	✓		
	T6 Jamming			✓
Device	T7 Loss, theft, disposal or damage	✓	✓	✓
	T8 Cloning SIM card	✓	✓	
	T9 Technical failure of device		✓	✓
Operating System	T10 Unauthorized device (physical) access	✓	✓	✓
	T11 Unauthorized Access	✓	✓	✓
	T12 Offline tampering	✓	✓	✓
	T13 Crashing			✓
Applications	T14 Misuse of Phone Identifiers	✓		
	T15 Electronic tracking/surveillance/exposure of physical location	✓		
	T16 Resource abuse			✓
	T17 Sensitive Information Disclosure (SID), Spyware	✓		
	T18 Corrupting or modifying private content		✓	✓
	T19 Disabling applications or the device			✓
	T20 Client Side Injection/ Malware	✓	✓	✓
	T21 Direct billing		✓	
	T22 Phishing	✓	✓	

3.3 Risk

The triplet used for the risk assessment of threats, which are associated with specific permission access rights (i.e. threats T14-T19, T21, T22) is: (asset, permission combination, threat).

Asset refers to the asset targeted by the threat. Permission combination refers to the permissions for the dangerous functionality required by the threat. The permission combination is the vulnerability the threat exploits. In turn, threat likelihood is valuated on the basis of: a) the likelihood of permission combination acceptance in the smartphone platform, b) the threat incident likelihood, i.e. statistics on threat incidents in the platform or previous incidents experienced by the user, and c) the relevant security control existence (e.g. Use of Mobile Device Management [20]). Given that the user has assessed the asset impact, the impact may be combined with the likelihood of the threat and the permissions acceptance, so as to calculate risk by forming the triplet: (asset impact, permission likelihood, threat likelihood) => Threat Risk

Risk assessment is calculated on the basis of a risk matrix [10]. Risk can be mapped as Low (0-2), Medium (3-5), or High (6-8). Since each threat is associated with specific security attributes, the relevant asset impacts are taken into account. For instance, when assessing the Risk of threat T17 ‘Sensitive Information Disclosure’ on

the data source 'Messaging', the disclosure impact value $Impact_{DS}$ (Messaging) is used as the asset impact, because the particular threat affects confidentiality.

Table 3. Risk matrix

Threat likelihood		**Low**			**Medium**			**High**		
Permission likelihood		**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Asset impact	**0**	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

For threats that cannot be associated with specific permissions, i.e. T1-T13, T20, such a triplet cannot be produced. In this case, threats are combined with specific assets, and their risk is calculated on the basis of asset impact and threat likelihood, where the likelihood is calculated based on threat incident statistics or previous incidents experienced by the user. This is done through a simple table (see Table 4).

Table 4. Simplified risk matrix

Threat likelihood		**Low**	**Medium**	**High**
Asset impact	**0**	L	L	M
	1	L	M	M
	2	L	M	H
	3	M	M	H
	4	M	H	H

4 Case Study: Risk assessment in Android

This section provides a demonstration of the proposed risk assessment method in the case of the Android platform. Android was selected because it is: a) popular smartphone platform holding the 52.5% of the smartphone market sales share in Q3 of 2011[8], b) open source and, hence, its security model details are publicly available, and c) well studied platform and statistics about its threats are available.

For the purpose of this case study a HTC Hero (Android version 2.1) owner is assumed, who holds a 'high' managerial position in the Pharmaceutical industry. The user identified two data types, i.e., personal data and business data. She provided data impact valuations as follows: $Impact_{UA}$(personal)=1, $Impact_{DS}$(personal)=2, $Impact_{MD}$ (personal)=2, $Impact_{UA}$(business)=2, $Impact_{DS}$(business)=4 and $Impact_{MD}$ (business)= 3. She chose not to assess network services and applications. She also assessed the replacement cost of the device as low, i.e. Impact(device)=1.

In addition, the user provided the following data: 1) the only smartphone security control enabled is the automatic password device lock, 2) she regularly discusses critical business issues over the carrier voice service, 3) she does not consider herself a technology or security savvy user, 4) no past security incident has ever come into her attention, 5) has noticed some delays in the device, 6) travels frequently in technology

'underdeveloped' country where fast 3G data connections are not available and, thus, her only way to connect to the internet is either through public free Wi-Fi hotspots, or expensive carrier network if one is not available, 7) has never updated the firmware, 8) she regularly installs applications while she is using public transport (trains, subway, etc). Finally, since Android's security is based on the user security consciousness (i.e. the user decides permission authorization during installation time in an all or nothing way [16]), the likelihood of a permission combination acceptance is estimated using Android application research and studies [5], [7].

For readability and space-limitations reasons, the case study focuses on risk that is due to threats T5, T10, T11, T13, T14, T17, T18, and T21.

T5 Eavesdropping. The user-identified the use of GSM voice services, in a carrier where UMTS is not supported. As a result, the possibility of abusing the discussion confidentiality is High [1] and the $Impact_{DS}$(GSM Service)=max{$Impact_{DS}$ (personal), $Impact_{DS}$(business)}=4. Risk is assessed as High (see Table 4).

T10 Unauthorized device (physical) access. The user has the automatic password device lock enabled, therefore this threat likelihood is Low. As physical access to a device affects all security attributes and may cause significant damage to the hardware itself, the total impact of the asset 'device' is the max value of the replacement cost and the relevant impact valuations for the data it holds. Therefore, Total_Impact(device) = max{Impact(device), $Impact_{DS}$(personal), $Impact_{DS}$(business), $Impact_{MD}$(personal), $Impact_{MD}$(business), $Impact_{UA}$(personal), $Impact_{UA}$(business)} = 4. Therefore, the threat risk is Medium (see Table 4).

T11 Unauthorized Access. The user is running an Android version that suffers by known security vulnerabilities. The vulnerabilities have been identified and patched by the device vendor without the user applying them. In addition, publicly available and stable (i.e. confirmed) source code exists, which can exploit the vulnerabilities[6]. The source code can be used by an attacker, so as to gain unauthorised access to the devise with administrator privileges. Thus, the threat likelihood is High. Since T11 may affect all security attributes but not the hardware itself, the $Impact_{DS,MD,UA}$(Device) is the max impact valuation of the data it holds, i.e. it equals with 4. As a result, the threat risk is High.

T13 Crashing. The user is running a buggy version of Android 2.1 that affects the device performance. An official fix (patch) for this vulnerability is available from the device vendor, thus, the threat probability is High. T13 affects the device's availability. The unavailability impact of the asset 'device' is the max value of the relevant impact valuations for the data it holds. Therefore, $Impact_{UA}$(device) = max {$Impact_{UA}$(personal), $Impact_{UA}$(business)}=2 and the threat risk is High (Table 4).

T14 Misuse of Phone Identifiers: This threat is associated with the triplet T1= <USIM Data, Open Network Sockets + Access Phone State, T9>. The likelihood of T14 is Low (~20%) [5]. The combination likelihood is, also, Low (≤35%) [7]. As a result, the following risk triplet is formed: <$Impact_{DS}$ (USIM Data), Low, Low>. Since the $Impact_{DS}$(USIM Data)=4 (i.e. max disclosure impact of associated data types - personal and business), the threat risk calculated from the triplet <4, Low, Low>,and, hence, it is 4 (Medium) (Table 3).

[6] http://www.exploit-db.com/exploits/15548/

T17 Sensitive Information Disclosure (SID), Spyware. Herein the call logs disclosure threat is examined. This is associated with the triplet: <UsageHistory, read the user's contacts data + Open Network Socket, T17_Call_Logs>. The permission combination, according to [7], is Low (≤16%), while statistics about the threat likelihood are not available. Thus, the risk triplet is: < $Impact_{DS}$ (UsageHistory), Low, N\A>, i.e. <4, Low, N/A>. As a result the risk varies from Medium to High.
T18 Corrupting or modifying private content. The removable storage corruption by junk file addition is herein examined. The permission involved in this threat is the 'Write to External Storage'. The threat triplet is: <Device, Write to External Storage, T18 Storage>. Relevant studies [7] have revealed the combination likelihood to Medium (≤50%), but additional data about the threat likelihood where unavailable at the time of publication. The threat triplet is: <$Impact_{UA}$(Device), Medium, N\A>. Thus, the threat risk is 3-5 (Medium).
T20 Client Side Injection/ Malware. The likelihood of this user downloading malware in her device is considered High, since: a) the user frequently installs applications in the device, b) user is not considered a security savvy one, and c) most smartphone malware are targeting Android (40% of mobile malware that was detected in Q3 of 2011[13]). As in T11, this threat may affect all security attributes but not the hardware itself, the $Impact_{DS,MD,UA}$(Device) is the max impact valuation of the data it holds, i.e. it equals with 4. Thus, the threat risk is High.
T21 Direct billing. Since the user frequently makes use of the carrier data connectivity, in order to connect to the Internet, malicious applications may abuse the Internet permission to incur direct costs to the user. The malicious application needs - apart from the permission to open network socket - access to the networking state, i.e. if the carrier data are being used. Hence, the involved triplet is: <USIMCard, Use Network Socket + Access Information about Networks, T21CarrierData>. The permission combination likelihood is High (≤86%)[7] [7], and the threat likelihood is also High. Thus, the threat triplet is: <$Impact_{MD}$(USIMCard), High, High>. As the $Impact_{MD}$(USIM Data)=3 (i.e. max modification impact of associated data types - personal and business), threat risk is calculated from the triplet <3, High, High> and thus it is 7 (High).

Table 5 summarizes the risk assessment of the threats included in the case study.

5 Conclusions

We have presented a risk assessment method that is tailored for smartphones. The method is compatible with established guidelines on risk assessment [10]. Nonetheless, contrarily to traditional risk assessment methods, which treat smartphones as a single entity, this method provides a more fine-grained valuation by: (a) dividing the device into various (sub)assets, (b) assessing smartphone-specific threats, and (c) taking into account the characteristics of a smartphone security model.

[7] Access to network state is granted to all Android applications without user intervention.

Table 5. Risk assessment results summary

Threat	Asset Impact	Permission Likelihood	Threat Likelihood	Risk
T5	ImpactDS(GSM Service) = 4	N\A	High	High
T10	Total_Impact(Device) = 4	N\A	Low	Medium
T11	$Impact_{DS,MD,\ UA}$(Device) = 4	N\A	High	High
T13	$Impact_{UA}$(Device) = 2	N\A	High	High
T14	$Impact_{DS}$(USIM Data) = 4	Low	Low	Medium
T17	$Impact_{DS}$(UsageHistory) = 4	Low	N\A	Medium-High
T18	$Impact_{UA}$(Device) = 2	Medium	N\A	Medium
T20	$Impact_{DS,MD,\ UA}$(Device) = 4	N\A	High	High
T21	$Impact_{MD}$(USIM Data) = 3	High	High	High

User input for (sub)asset impact is based on a two-dimensional data taxonomy. The data analysis takes place transparently to the user and it leads to a 'personalised' risk assessment, as opposed to other smartphone-oriented methods, which use mainly expert opinions [6], [21]. The level of input detail varies according to user skill [14] - this may indeed affect the quality of results - but our approach requires minimum input, i.e. the data impact valuation. The method could be potentially used in order to extend an information risk assessment method to include smartphone-specific threats, as its theoretical basis is compatible with best practices, i.e. ISO27005 [10].

This is used in combination with a threat list to conduct risk assessment. The list was compiled by extending existing threat lists of smartphone literature. For threat assessment, risk triplets are introduced, which makes the approach novel. They use application permissions as the attack vector, associating assets to threats and permission combinations. Risk is, then, assessed as a combination of asset impact and threat likelihood. Finally, a demonstration of the proposed assessment method is provided, via a case study based on the Android platform.

It should be noted that generic conclusions for specific threats cannot be drawn by 'high' risk valuations of a hypothetical, single case. Risk is highly affected by the valuation of impact, which is a parameter that varies among different users. However, our method can also be applied in other smartphone platforms with permission-based security models (e.g. Symbian, Windows Phone, etc.), as well as in other platforms (e.g. iOS, BlackBerry, etc.) with some minor adjustments. For instance, risk triplets can be created by examining API library combinations of applications that exist in application repositories.

Future research may aim for an extended review of threats and vulnerabilities, along with an analytical dictionary of permission combinations. This will allow a more detailed threat assessment, based on past incidents or statistics, the presence of vulnerabilities or controls, analyzed on a per threat basis. We may also provide explanatory impact valuation tables and relevant questionnaires, which are appropriate for smartphone users.

Acknowledgements. This research has been co-funded by the European Union (ESF) and Greek national funds, through the Operational Program "Education and Lifelong

Learning" of the National Strategic Reference Framework (Program HERACLEITUS II: Investing in knowledge society through the European Social Fund).

References

1. Becher, M., Freiling, F., Hoffmann, J., Holz, T., Uellenbeck, S., Wolf, C.: Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In: Proc. of the 2011 IEEE Symposium on Security and Privacy (SP '11), pp. 96—111, IEEE Computer Society, USA (2011)
2. Caldwell, T.: Smart security. Network Security, 2011(4), 5—9 (2011)
3. Dietz, M., Shekhar, S., Pisetsky, Y., Shu, A., Wallach, D.: Quire: lightweight provenance for smart phone operating systems. In: 20th USENIX Security Symposium, USA (2011)
4. Dlamini, M., Eloff, J., Eloff, M.: Information security: The moving target. Computers & Security, 28(3-4), 189—198 (2009)
5. Enck, W., Octeau, D., McDaniel, P., Chaudhuri, S.: A study of android application security. In: Proc. of the 20th USENIX conference on Security (SEC'11), pp. 21—21, USA (2011)
6. Hogben, G., Dekker, M. :Smartphones: Information security risks, opportunities and recommendations for users. Technical Report, ENISA (2010)
7. Felt, A.P., Greenwood, K., Wagner, D.: The effectiveness of application permissions. In: 2nd USENIX Conference on Web Application Development (WebApps 11), pp. 75—86 (2011)
8. Gartner: Market Share: Mobile Communication Devices by Region and Country, 3Q11. Technical Report (2011)
9. Grace, M., Zhou, Y., Wang, Z., Jiang, X.: Systematic Detection of Capability Leaks in Stock Android Smartphones. In: Proc. of the 19th Network and Distributed System Security Symposium (NDSS'12) (2012)
10. ISO/IEC: Information technology – Security techniques - Information security risk management. ISO/IEC 27005:2008, 1st edition (2008)
11. Jansen, W., Scarfone, K.: Guidelines on Cell Phone and PDA Security. Recommendations of the National Institute of Standards and Technology, Special Publication 800-124 (2008)
12. Jeon, W., Kim, J., Lee, Y., Won, D.: A Practical Analysis of Smartphone Security, In: Smith, M., Salvendy, G. (eds.) Human Interface and the Management of Information. Interacting with Information, LNCS 6771, pp.311—320, Springer (2011)
13. Kaspersky Labs: IT Threat Evolution: Q3 2011, http://www.securelist.com/en/analysis/204792201/IT_Threat_Evolution_Q3_2011
14. Ledermüller, T., Clarke, N.L.: Risk Assessment for Mobile Devices. In: Furnell, S., Lambrinoudakis, C., Pernul, G. (eds.) Trust, Privacy and Security in Digital Business, LNCS 6863, pp. 210—221, Springer (2011)
15. Mylonas, A.: Smartphone spying tools. MSc Thesis, Royal Holloway, University of London (2008)
16. Mylonas, A., Dritsas, S., Tsoumas, B., Gritzalis, D.: Smartphone Security Evaluation: The Malware Attack Case. In: Samarati, P., Lopez, J. (eds.) International Conference on Security and Cryptography (SECRYPT'11), pp. 25—36, SciTePress (2011)
17. Nachenberg, C.: A Window Into Mobile Device Security. Technical Report, Symantec Security Response (2011)
18. Oppliger, R.: Security and Privacy in an Online World. Computer, 44 (9), 21—22 (2011)
19. OWASP: Top 10 Mobile Risks, http://www.owasp.org/index.php/WASP_Mobile_Security_Project
20. Phillip Redman, John Girard, L.: Magic quadrant for mobile device management

software. Technical Report G00211101, Gartner (2011)
21. Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y, Dolev, S., Glezer, C.: Google Android: A Comprehensive Security Assessment. IEEE Security and Privacy, 8 (2), 35—44 (2010)