Mobile Device Security, Management of Personal and Business Privacy

Oleg Mikhalsky, Ekaterina Pshehotskaya
Polytechnic University
Moscow, Russia
oleg@mikhalsky.ru, Pshehotskaya@gmail.com

***Abstract*—This paper is concerned with arising problems on security and privacy of personal data on mobile devices. We consider various classifications of mobile devices and their software services as well as types of user behavior regarding the involved security risks of unauthorized access to the data stored both locally and remotely. We also categorize potential threats that originate from compromised data of different classes. Based on provided categorization we discuss the means to generalize user patterns and evaluate the corresponding vulnerability level.**

I. Introduction

The ongoing advance of computer technologies has already resulted in almost total civilization dependence on vast amounts of stored data and the means of processing it. The ever-progressing hardware and software capabilities already overcame two barriers on the way to information society, namely: availability/affordability and usability/safety.

The first obstacle meant the scarcity or absence of data processing infrastructure, and, therefore, the prohibitively high obtaining costs for both electronic devices and program counterparts. These circumstances initially resulted in relative safety of data, since most of the users where sparse and belong to small privileged groups. The growing abundance of affordable hardware and widening of communication channels like Bulletin Board Systems increased the number of users beyond easy individual tracking and made possible fast regional propagation of early computer malware in the form of primitive viruses and worms.

At that stage the threat was limited by the second obstacle in the form of poor usability of computer applications that required special qualification to operate, since improper use could potentially corrupt user data. However, the user population increased with the gradual improvement of program interfaces and data safety mechanisms, both preventing unintentional data damaging actions. The spreading of personal computers and broadening of Internet access gave rise to various cyber-crimes. These cyber-crimes where initially profitable only when aimed at large organizations, mostly financial and governmental ones, due to low capabilities of mass processing, required for the bulk of ordinary user accounts. First malicious activity deliberately targeted to the common users was email spamming, often coupled with fishing in the form of "Nigerian letters" and other harmful and deceptive forms of social engineering techniques. With the onset of Internet banking and commerce more dangerous crimes like identity theft became commonplace and induced the countermeasures like governmental cyber-law enforcements and private cyber-security companies, with the latter often inheriting and superseding early vendors of antiviral software.

At the current moment, the data growth and devices production are unbounded. The manufactured devices with WAN access are somewhat outnumbering human population. Such phenomenon with epic proportions of standardized communication nodes usually termed as "Internet of things" (IoT) become the third barrier to the next generation of information society. The main issue of this remaining barrier is essentially the vulnerability of majority of devices, lacking due to simplicity and cost reduction any plausible means to provide reliable authentication of incoming connections. The range of the devices spans from network-accessible digital modules with MQTT-protocol for primitive sensors (e.g. house-hold Wi-Fi digital thermometers) to embedded single-board computers (e.g. Raspberry Pi) for more sophisticated consumer electronics like refrigerators, washing machines and TV-sets. Due to standardization of both machine architecture and communication protocols every node can serve as a breaching point for malicious cyber activity. For example, it is well established fact that smart TV sets already carried out unprecedented unauthorized audio-recordings even without notification of owners [1]. The same activity was revealed for smartphones detecting low noise of TV activation and collecting statistics on viewed channels. This kind of technology is known as cross-device tracking via audio beacons [2] and is actively developed by the corresponding industry leader SilverPush [3] and its competitors like Drawbridge, and Flurry as well as Adobe.

Thus, the modern technologies gave rise to wide diversity of threats to user data with multiple vectors of attack. Therefore, it is desirable to provide the methodology for estimation of risks to user data based on specifications of user devices, services and behavior. We aim to construct such methodology in the following sections.

II. Estimation of device data security

A. Threats to user data

There are several ways for unauthorized persons potentially to get access to the user data. These ways vary in the scale and complexity as well as in the associated expenses and frequencies of occurrence. The common vectors of unauthorized access are

- Theft of physical device with user data.

- Duplication of user data via malware applications installed locally on the device.
- Duplication of user data via interception of communication channels.
- Duplication of user data replicas via breach in the remote storage.

The theft is the most common and identifiable crime affecting electronic devices. The studies of Consumer Reports indicate that only in USA in 2013 about 3.1 million consumers fell victims to smart phone theft [4] nearly doubling the same annual indicators for 2012. In 2014 the number of reported thefts dropped to 2.1 million [5] due to deterring measures like locks and kill-switches introduced by some but not all manufacturers. Despite the trend changes to decline the overall number of device thefts all over the world remains high and can be roughly estimated in tens of millions per year. According to Lookout Mobile Security [6], 44 percent of all lost mobile devices are left in public places, while 14 percent are taken from a house or car, and 11 percent are pick-pocketed. Moreover, the major aspect of the device theft shifts from data loss to data compromise, since it much easier to recover data from a backup than to reliably purge data from a media before it undergoes unauthorized replication.

The less obvious user data compromise can be a result of malware applications installed on the device. These applications act either automatically, sniffing data by search templates or provide clandestine remote control over the device. Usually this malware is distributed on various software depot cites and comes under the guise of well-known applications with license protection removed. However, it is not uncommon to get a malware from official stores, as it slips through security screening. According to the recent Mobile threat report [7] by Intel Security, the three months‘ client-side scans of App Stores detected about 9 million of malware and additionally 9 millions of suspicious applications of the total 150 million of processed applications. Over six months there was 37 million of malware applications detected on various App Stores.

In extreme cases the suspicious activity can be even the part of pre-installed operating system as noted in [8], [9], for scanning storage media and sending data to third party servers. There are proofs of concept that the applications utilizing the most of the device capabilities can even jump over airgaps of naive isolation by resorting to acoustic means of communication with other devices [10], [11]. The modern high technology malware consists of confirmed advanced designs like Stuxnet [12], Flame [13], Duqu [14], Downadup as well as EquationDrug and GrayFish [15]. The analysis of these designs and their functionality shows that the future malware will employ leaking emanations, including but not limiting to unintentional radio or electrical signals, sounds, and vibrations with potential to defeat TEMPEST protective measures. On one hand, such high-end malware being quite certainly an expensive government-approved weapon of cyber-warfare is unlikely to possess a direct threat to ordinary users. On other hand, the weapon itself like any digital data can be lost or stolen, reverse-engineered and openly distributed (like Stuxnet), thus compromising control over its use.

Another not obvious attack is aimed to intercept sensible data travelling through device communication channels. This attack is usually carried out through the means of hacked or maliciously organized Wi-Fi hotspots with open access and compromised HTTPS protocol [16]. Almost anyone establishing such connection has their traffic compromised. The only exception are the advanced users, applying VPN-tunnels to secured servers. In rare cases, since Wi-Fi is essentially a radio signal, the traffic is passively intercepted by special purpose systems (e.g. see [17]). However, such data intelligence tools are expensive and legally restricted, thus, quite uncommon.

Breach of data storage systems is the most dangerous threat, since it simultaneously compromises massive amount of user accounts. Per Gemalto, their Breach Index reports [18] the publicly disclosed number of breached user records exceeded 1 billion and totaled 1,023,108,267 in 2014. The overall number of breached records reported from 2013 to current day is close to six billion [19]. Among these statistics, only about 4 percent of breaches where secured i.e. stolen data was encrypted, and thus, rendered useless to the thieves. Since the breach occurs at the server-end, the user is unable to prevent data compromise even by ideally protecting his client-end device and ideally conforming to security policies for it. This circumstance serves as another example of mutual opposition of safety and security, since data safety require to place multiple easily accessible replicas on remote storage services whereas data security dictates to minimize the number of heavily encrypted copies. The statistics of Gemalto confirm that most service providers deeply favor data safety over data security.

B. The estimation of risks to user data

1) Device classification: At the current age of worldwide communications, the user data is nearly always exposed to risks by various degree, depending on the user device type, user applications and services as well as the qualities of data itself. In this part of the paper we consider the following qualities categorizing personal electronic devices:

- Cost.
- Portability.
- Diversity.
- Controllability.
- Hardware security measures.

The device cost is one of the top properties contributing to the risk of theft. It is obvious that the expensive top-tier state-of-art devices attract more unhealthy attention that aging low and medium cost counterparts. For example, the study on smartphones thefts conducted by the Behavioural Insights Team of Home Office [20] reveals that various manufacturer brands and product models differ greatly in likeliness of being stolen. The likeliness ratio is presented on the Fig. 1–2. The values on these figures are the ratio of all thefts of a model both targeted (the phone has been snatched) and untargeted (the phone has been stolen in a burglary) to the share of untargeted thefts. The statistics varies with time and should be updated at regular time intervals of about quarter of a year, or even monthly, if circumstances permit. The statistics also indicates status of a certain smartphone model, since the iPhones are

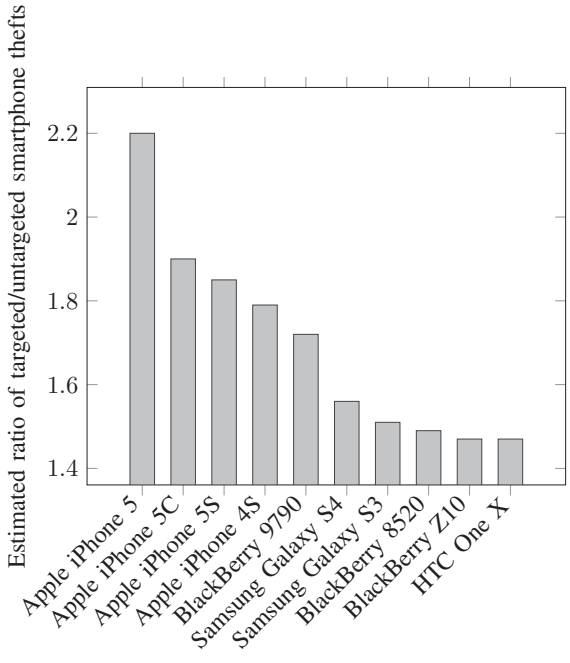

Fig. 1. Likeliness of deliberate smartphone thefts

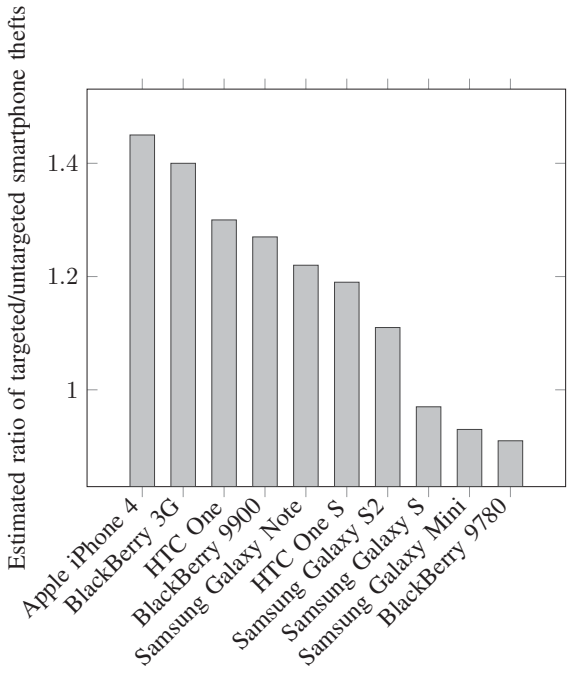

Fig. 2. Likeliness of deliberate smartphone thefts, cont'd

stolen more deliberately that other brands, while Apple having lesser market share than the Samsung brand.

The portability essentially means the size-weight-operating time characteristics of the device. It is obvious that small devices, like smartphones and tablets or portable media storages are easier both to lose and steal than large notebooks, not mentioning tabletop PCs and server racks. However, relatively large devices are usually having modular structure that can be dismantled on site for retrieval of data sensitive components like HDD and SSD units or DRAM modules in case of Cold Boot attack.

The diversity is indicating how rich the product line is. In other words, it shows the variability of the product architecture in aspects of implemented hardware, firmware and software. If the product line is extremely small, then the devices are more often aimed by hardware- and firmware-specific attacks. The products with the same single architecture can be more resistant to exploits, but once breached they expose to the threat all users of the whole product line. The products with varying and diverse elements of architecture can be less resilient to attacks, but one breached product can compromise only the respective part of users. Moreover, users can select another product of the line without any changes in usability. However, some architecture flaws can be common for a global-wise range of device models, regardless of their manufacturers. For example, newly discovered "Quadrooter" set of vulnerabilities in Qualcomm chipsets [21] affect more than 900 million of android operated smartphones and tablets gaining the root-level access.

The controlability indicates how complete the user control over the device is. For example, is an operating system allows user by default to operate with a file system, or require a custom jail-break, effectively terminating the warranty on the device. The hardware security measures are comprised of fingerprint sensors as well as a circuitry protection against physical intrusion. However, the fingerprint lock are susceptible false positive acknowledgements of artificial inputs.

2) Types of user behavior: We also consider user behavior, especially Internet-activity, since it also contributes to security risks. Per 2014 study of Consumer Reports, only 36 percent of smart-phone users set a four-digit PIN screen lock, 14 percent install antivirus application, 11 percent implement multidigit PIN or unlock pattern, 8 percent install data purge software and 7 percent utilize encryption. In contrast, 34 percent of users did not apply any of these measures. However, the proper and secure smart-phone handling is only a part of risk mitigation policies, since it reduces only two threats, namely: device theft and malware data theft. Two remaining risks essentially depend on user Internet-activity. Thus, the user behavior can be divided into following categories:

- Local device handling.
- Network handling.
- Remote services handling.

The network handling category indicates, how strict or relaxed are the user choices to connect to unknown communication nodes. Currently the most common are Wi-Fi and Bluetooth nodes. The recent Kaspersky Lab report [22] shows that among 31 million of analyzed Wi-Fi hotspots almost 22 percent lack any security and additional 2.7 percent has the obsolete WEP-protection, which is easy to defeat. Another research [23], conducted by Norton (Symantec) reveals that 61 percent of 9135 respondents completely disregard risks of public Wi-Fi networks, considering their information to be safe. This study indicates that exaggerated trust to hotspots is somewhat age-related, since Millennials trust public Wi-Fi more (68

percent) that users over age of 55 (55 percent). Nevertheless, the recent survey [24] of 1.516 respondents conducted by ISPreview.co.uk discovered that users prefer mobile broadband 3G/4G over public Wi-Fi hotspots with respective percentage of 72 and nearly 21. However, even mobile broadband communications can be compromised via the use of fake base stations delivering a man-in-the-middle (MITM) attacks [25].

Remote online services provide user with multitude of applications for purposes varying from entertainment and document editing to scientific research and online banking. The distinctive feature for all online services is the massive amount of stored user data. These amounts of data make services quite attractive targets to hack. Despite even corporate-grade security measures, the number of large-scale breaches increase every year. Gemalto reveals 1541 reported breaches for 2014 [18], and 1673 incidents during 2015 [26] along with 974 breaches for the first half of 2016 [27]. The breached organizations belong to both commercial and governmental sectors. Among them are U.S. Healthcare Insurers database, U.S. Office of Personnel Management (OPM), Philippines Commission on Elections, Mexican Voters, Turkish General Directorate of Population and Citizenship Affairs, as well as JP Morgan Chase, AliExpress and Sony Pictures Entertainment. Per recent Statista report [28] the most iconic of all breaches dates back to 2013 and results in over billion records stolen from Yahoo, not accounting for additional 500 million records compromised in the separate breach. The cumulative chart on number of compromised records due-to large-scale data breaches is presented on Fig. 3 The lesser services can suffer breaches without even publicly reporting them. Therefore, the users are advised to carefully select the size and content of their digital footprint in the global network. It is plausible to assume that the more accounts user is involved in, the greater is the risk to the corresponding user data. However, the user is unable to completely remove his digital footprint, since some personal information is gathered by government agencies and stored mandatory and involuntary. Moreover, the technology of cross-authorization for social networks, when main-account credentials of one network permit the access to account of another network, significantly reduce the overall security in case of main-account compromise.

There are also many habits, which indirectly impact the risks for user data. The Great Britain Home Office report on the mobile phone theft ratio [20] reveals dependence of theft frequency on location (see Fig. 4–5). Thus, the most of thefts in London unsurprisingly occur in pubs and clubs (17 percent), while the least thefts happen in educational venues (2 percent). The Lookout report [29] basically somewhat disagree to the ratios, placing restaurants (16 percent) on top of likely-theft locations (see Fig. 6). So, the habit of visiting specific locations implicitly affects the overall risks to data security. Even the carrying place of the device make a difference to the probability of theft. For example, a theft from a pocket is less likely that a theft from a bag [20] (Fig. 7).

3) Types of user data: The risks to user data depend not only on storage and communication infrastructure, but also on the type of data itself. Per Norton survey [23], the users are most concern of the following:

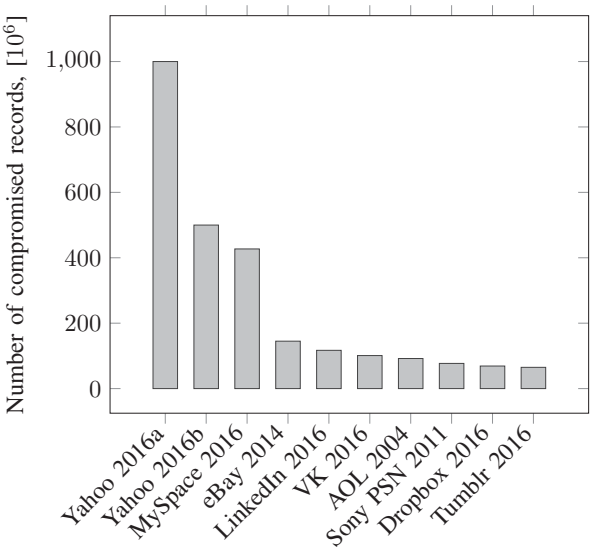

Fig. 3. The number of compromised records in large-scale data breaches since 2013

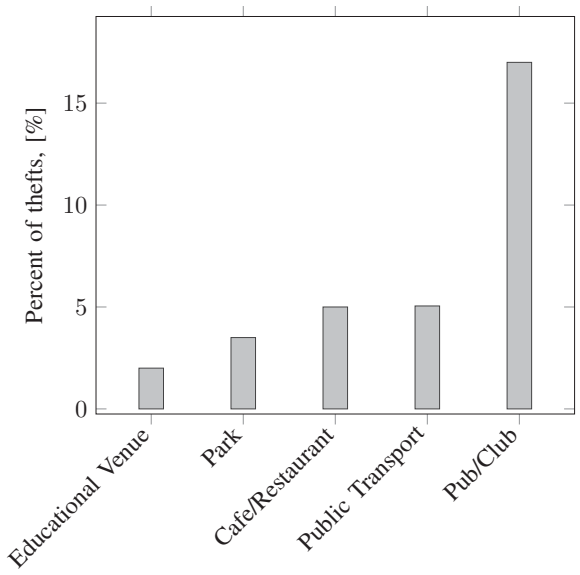

Fig. 4. Percentage of London mobile phone thefts by location

- Theft of user information (85 percent).
- Unauthorized access to financial information (85 percent).
- Infection with malware (84 percent).
- Unauthorized access to personal photos/videos (72 percent).

These indicators agree with the Gemalto findings [26], which state the following types of compromised data (in percent of annual breach incidents):

- Identity data (53 percent).
- Financial access data (22 percent).

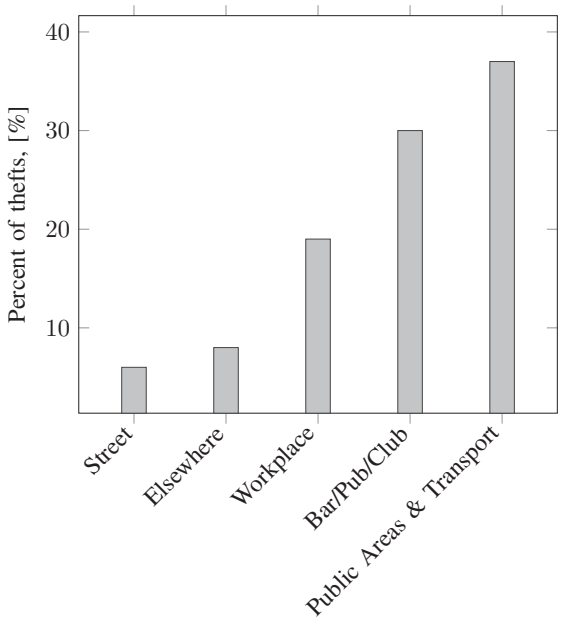

Fig. 5. Percentage of England and Wales mobile phone thefts by location

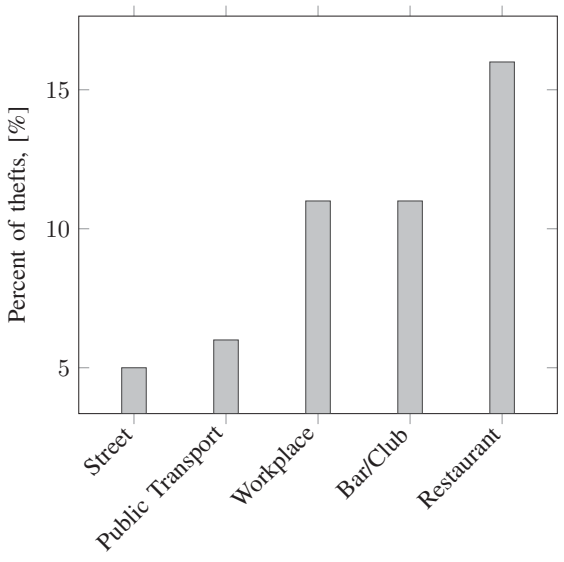

Fig. 6. Percentage of US mobile phone thefts by location

- Account access credentials (11 percent).
- Existential data (11 percent).
- Nuisance data (4 percent).

The more detailed data user-concerned types are considered in the Lookout study [30]. The published results are presented on the Fig. 8 and confirm Gemalto and Norton surveys. The SSN, Driver‘s License and Passport Numbers as well as Health Insurance ID constitute user digital identity. The Bank Account Number, Credit Cards Numbers, Tax Information are related to financial data. Login Credentials are self-explanatory and existential data is represented by Email Address and Phone Number. These types of data allow one to assume the user

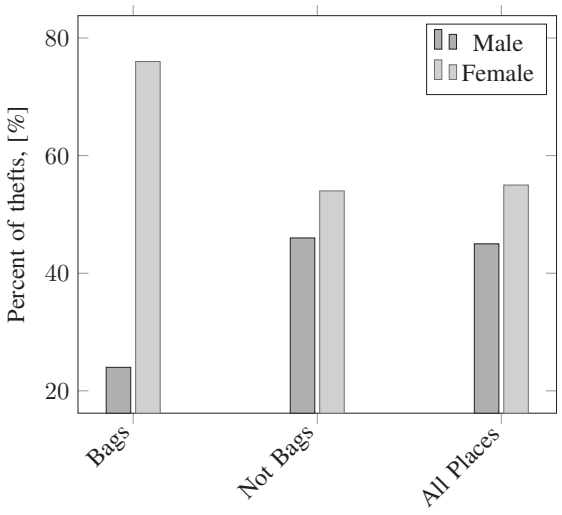

Fig. 7. Proportion of London mobile phone thefts by gender and carrying place

risk types, considered in the following subsection.

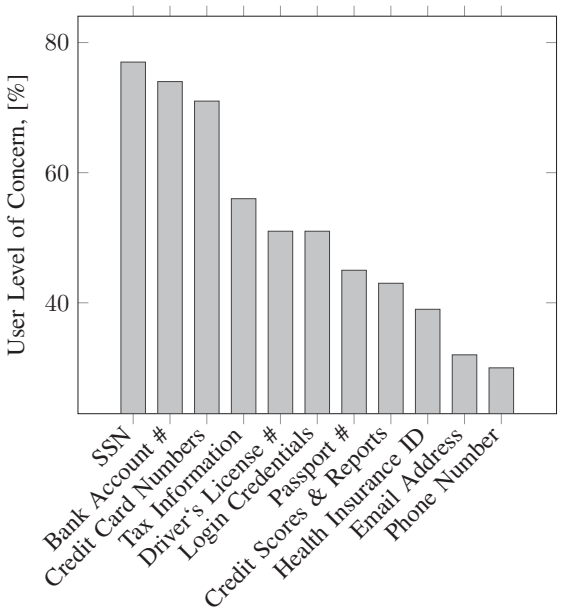

Fig. 8. User concerns on types of would-be compromised data

4) Classification of risks and losses: Each type of above mentioned data corresponds to multiple risks of various severity to the user if compromised. It is naturally to classify risks on the scale of the possible harm as follows:

- Identity theft.
- Financial losses.
- Account theft.
- Mundane losses.

The identity theft is the most complex and heavy risks one can experience. This risk includes all lesser risks from financial to

mundane losses and requires much effort for its mitigation, since it is no less than a user impersonation. The exposed and compromised data includes document numbers and personal identifiers, logins and passwords as well, as the geolocations, social connections as well as the bulk of behavior examples and personal history. Thus, the affected person should prove his identity, regain it and minimize the responsibility for fraudulent actions conducted by perpetrators allegedly on his behalf. However, usually it is impossible to completely nullify the alleged responsibility and corresponding losses, for example, the financial or reputation ones. In worst case scenario, the impersonated user can face legal prosecution. The partial identity theft can lead to financial loses, since the corresponding institutions are legitimately unwilling to compensate anyone for seemingly authorized expenses. However, the de-facto standard of financial transaction contains the two-factor authentication, which is very robust against the mid-profile attacks lacking large infrastructural support. The account theft is an interception of control for non-financial user accounts, when the primary damage comes in the form of reputation losses due to leakage of private information like photos and memos. Moreover, account theft can serve an intermediate stage for a higher-profile attack via mining within collected bulks of user data. The mundane losses are often underestimated, since they have limited impact on finances and reputation. For example, the failed account remains a nuisance, since the user should spend time to change password or multiple passwords if the single one is used across several accounts. The mundane losses include the compromise of existential data, like geopositioning history, e-mail addresses and phone numbers, exposing the user to additional spam-messages. The mundane losses should not be discarded easily, because they accumulate up to critical level and start to pose higher-tier risks.

C. Mathematical model of risk estimation

As we established in the previous section, the risks depend on user hardware and software preferences, user digital footprint, overall network and social behavior as well as the types of device-stored data. However, it is impossible to estimate absolute probabilities of risks, since there is no underlying detailed raw personal statistics for such prediction. To resolve this issue, we propose to introduce a baseline representing a profile of a generic average user and estimate risks relative to it. Without restricting the generality, we select as an i-th baseline $p_{b,i}$ the risk $r_{i,\cdot}$ with average probability (or frequency of occurrence) $p_{i,\cdot}$ of all N_i risks in i-th category:

$$p_{b,i} = \frac{1}{N_i}\left(p_{i,1} + p_{i,2} + \cdots + p_{i,N_i}\right) = \frac{1}{N_i}\sum_{j=1}^{N_i} p_{i,j}. \quad (1)$$

Thus, the actual j-th risk corresponding to i-th category $r_{i,j}$ of user profile has the amplification factor $a_{i,j}$ with respect to appropriate baseline $p_{b,i}$:

$$a_i = \frac{p_{i,j}}{p_{b,i}}. \quad (2)$$

Therefore, the overall increase of risk occurrence can be estimated as the product of amplification factors across all K risk categories:

$$R = \prod_{k=1}^{K} a_k. \quad (3)$$

The value R indicates how great the risk for specified user profile is, in comparison with baseline average-risk profile. For example, the user, who owns Apple iPhone 4 and visits bars in the USA, it is 2.3 times likely to experience theft than for an average user. On other hand, the user, who owns iPhone 5C and visits bars and clubs in UK, is 5.9 times likely to experience theft than for an average counterpart with Samsung Galaxy S. The same technique can be applied to statistics on data breaches and records compromising. Thus, average user is experiencing 10 times more potential vulnerability risks if creating an account at Yahoo than creating an account at eBay. In this estimation, we assume that all web-services have the roughly equal level of breach-resistance and the frequency of attacks is proportional to the number of accounts. From this point of view, the user of a small 1000-account website with the same level of protection as of Yahoo, is exposed to much lesser risk, since the target is much smaller. We emphasize that the most accurate user risk evaluation model should incorporate the results of independent regular security audits for the architecture of web services. This, indeed, is not possible due for obvious reasons, including concerns of disclosing security imperfections and commercial secrets. Moreover, the detailed audit of large program systems is both time-consuming and expensive. We can construct risk models based of linear systems, where various characteristics of user behavior are summed with a priori unknown weights resulting in normalized risk values. These weights can be calculated from least squares problem for a known risk values, computed from e.g. frequencies of user data compromises. However, the bulk of data on personal cases of data compromise are unavailable for use outside law-enforcement agencies. Therefore, we can only rely on published statistics and front-end observations of web services, when outlining the technique for risk estimation.

III. Conclusion

In this paper, we considered classifications of various threats and their different dependencies. We outlined the simple approach for estimation of user relative risks. To our belief, the proposed technique can be successfully used if supplemented by detailed statistical data on above mentioned aspects of data compromise.

References

[1] Harris, S. Your Samsung SmartTV Is Spying on You, Basically. The Daily Beast, 06.02.15. http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html

[2] Ha, A. SilverPush Says It's Using "Audio Beacons" For An Unusual Approach To Cross-Device Ad Targeting. Tech Crunch, 24.06.2014. https://techcrunch.com/2014/07/24/silverpush-audio-beacons

[3] Goodwin, D. Law & Disorder Beware of ads that use inaudible sound to link your phone, TV, tablet, and PC. ArsTechnica, 13.11.2015. https://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc

[4] Tapellini, D. Smart phone thefts rose to 3.1 million in 2013. Industry solution falls short, while legislative efforts to curb theft continue. Consumer Reports, 28.05.2014. http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

[5] Deitrick, C. Smartphone thefts drop as kill switch usage grows but Android users are still waiting for the technology. Consumer Reports, 11.06.2015. http://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm

[6] Eadicicco, L. People Are Willing To Go To Extreme Lengths To Retrieve Their Stolen Smartphones. Business Insider, 07.05.2014. http://www.businessinsider.com/smartphone-theft-statistics-2014-5

[7] Snell, B. Mobile Threat Report. What's on the Horizon for 2016. Intel Security, 01.03.2016. https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

[8] Once again on Xiaomi phones and struggle against them. Updated. HabraHabr, 27.01.2017. [in Russian] https://habrahabr.ru/post/320612

[9] Misterious Backdoor is revealed on Xiaomi Android smartphones. Security Lab, 16.09.2016. [in Russian] http://www.securitylab.ru/news/483861.php

[10] Goodwin, D. Scientist-developed malware prototype covertly jumps air gaps using inaudible sound. Malware communicates at a distance of 65 feet using built-in mics and speakers. Ars Technica, 02.12.2013. https://arstechnica.com/security/2013/12/scientist-developed-malware-covertly-jumps-air-gaps-using-inaudible-sound

[11] Wisneski, C. Ultrasonic Local Area Communication. MIT. http://alumni.media.mit.edu/ wiz/ultracom.html

[12] Zetter, K. Law & Disorder How digital detectives deciphered Stuxnet, the most menacing malware in history. Ars Technica, 11.07.2011. https://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history

[13] Goodwin, D. Spy malware infecting Iranian networks is engineering marvel to behold. Ars Technica, 29.05.2012. https://arstechnica.com/security/2012/05/spy-malware-infecting-iranian-networks-is-engineering-marvel-to-behold

[14] Brodkin, J. Spotted in Iran, trojan Duqu may not be "Son of Stuxnet" after all. Ars Technica, 27.10.2011. https://arstechnica.com/business/2011/10/spotted-in-iran-trojan-duqu-may-not-be-son-of-stuxnet-after-all

[15] Zetter, K. How the NSA's Firmware Hacking Works and Why It's So Unsettling. Wired, 22.02.15. https://www.wired.com/2015/02/nsa-firmware-hacking

[16] Geier, E. Here's what an eavesdropper sees when you use an unsecured Wi-Fi hotspot. PCWorld, 28.06.2013. http://www.pcworld.com/article/2043095/heres-what-an-eavesdropper-sees-when-you-use-an-unsecured-wi-fi-hotspot.html

[17] Wi-Fi Interception System (SCL-2052). Shoghi. http://www.shoghicom.com/wifi-interception.php

[18] 2014 Year of Mega Breaches & Identity Theft. Gemalto. http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf

[19] breachlevelindex.com http://breachlevelindex.com

[20] The Behavioural Insights Team. Reducing Mobile Phone Theft and Improving Security. Home Office, 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/390901/HO_Mobile_theft_paper_Dec_14_WEB.PDF

[21] Khandelwal, S. Warning! Over 900 Million Android Phones Vulnerable to New 'QuadRooter' Attack. The Hacker News, 07.08.2016. http://thehackernews.com/2016/08/hack-android-phone.html

[22] Jackson, M. Kaspersky Lab Reports 25% of WiFi Internet Hotspots are Unsecured. ISP News, 28.11.2016. http://www.ispreview.co.uk/index.php/2016/11/kaspersky-lab-reports-25-wifi-internet-hotspots-unsecured.html

[23] Jackson, M. Norton – Only 42% of People Can Tell if a Wi-Fi Network is Secure or Not. ISP News, 29.06.2016. http://www.ispreview.co.uk/index.php/2016/06/norton-42-people-can-tell-wi-fi-network-secure-not.html

[24] Jackson, M. Study – Mobile Broadband Still More Popular than Risky Public Wi-Fi. ISP News, 25.10.2016. http://www.ispreview.co.uk/index.php/2016/10/study-mobile-broadband-still-popular-risky-public-wi-fi.html

[25] Borgaonkar, R., Shaik, A. et al. LTE and IMSI catcher myths. BlackHat. https://www.blackhat.com/docs/eu-15/materials/eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths-wp.pdf

[26] 2015. The Year Data Breaches Got Personal. Gemalto. http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf

[27] 2016. It's All About Identity Theft. Gemalto. http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf

[28] Richter, F. Latest Yahoo Hack Is the Largest Data Breach To Date. Statista, 15.12.2016. https://www.statista.com/chart/5983/data-breaches

[29] Phone Theft in America. Breaking down the phone theft epidemic. Lookout, 2014. https://transition.fcc.gov/cgb/events/Lookout-phone-theft-in-america.pdf

[30] Identity Theft in America. Shedding light on an evolving epidemic. Lookout, 2016. https://info.lookout.com/rs/051-ESQ-475/images/lookout-breach-identity-protection.pdf