IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 15, 2016, accepted January 23, 2017, date of publication February 17, 2017, date of current version March 15, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2665640

Mobile Social Networking Under Side-Channel Attacks: Practical Security Challenges

ALEKSANDR OMETOV[1], ALLA LEVINA[2], PAVEL BORISENKO[2], ROMAN MOSTOVOY[2], ANTONINO ORSINO[1], AND SERGEY ANDREEV[1]

[1]Tampere University of Technology, 33720 Tampere, Finland
[2]ITMO University, 191002 Saint Petersburg, Russia

Corresponding author: A. Ometov (aleksandr.ometov@tut.fi)

ABSTRACT Mobile social networks (MSNs) are the networks of individuals with similar interests connected to each other through their mobile devices. Recently, MSNs are proliferating fast supported by emerging wireless technologies that allow to achieve more efficient communication and better networking performance across the key parameters, such as lower delay, higher data rate, and better coverage. At the same time, most of the MSN users do not fully recognize the importance of security on their handheld mobile devices. Due to this fact, multiple attacks aimed at capturing personal information and sensitive user data become a growing concern, fueled by the avalanche of new MSN applications and services. Therefore, the goal of this work is to understand whether the contemporary user equipment is susceptible to compromising its sensitive information to the attackers. As an example, various information security algorithms implemented in modern smartphones are thus tested to attempt the extraction of the said private data based on the traces registered with inexpensive contemporary audio cards. Our obtained results indicate that the sampling frequency, which constitutes the strongest limitation of the off-the-shelf side-channel attack equipment, only delivers low-informative traces. However, the success chances to recover sensitive data stored within a mobile device may increase significantly when utilizing more efficient analytical techniques as well as employing more complex attack equipment. Finally, we elaborate on the possible utilization of neural networks to improve the corresponding encrypted data extraction process, while the latter part of this paper outlines solutions and practical recommendations to protect from malicious side-channel attacks and keep the personal user information protected.

INDEX TERMS Mobile social networks (MSNs), information systems security, side-channel attacks, social networking services, neural networks.

I. INTRODUCTION

The rapidly growing numbers of mobile devices as well as ''social'' multimedia applications and services demand for direct connectivity means between users to offload the infrastructure of a network operator, which is possible over a range of wireless technologies [1]. This rich heterogeneous connectivity fuels the novel networking paradigm, named mobile social networks (MSNs), where the connectivity and data sharing patterns among users are based on their social contacts and relationships [2], [3]. According to Sandvine Global Internet Phenomena Report, MSNs had a 22%-share of mobile traffic in the US and this figure has been growing tremendously over the past decades.[1] Broadly, MSNs are often delay-tolerant and may be characterized by intermittent connectivity as well as limited network capacity, thus having difficulty to support the increasing user data rate requirements [4].

One of the first works that concentrate on MSNs from the perspective of coupling the functionality of conventional social networks with the features of mobile communications was summarized in [5]. In a nutshell, the authors proposed that the users may exploit their social contacts in order to improve the networking efficiency from a user-centric perspective. Another line of research on MSNs considers conventional social networks with a centralized control unit, where the data may be acquired directly *through* mobile devices in case the central node fails [6]. In these situations, the devices in proximity may communicate by utilizing short-range radio technologies (e.g., device-to-device communications – D2D) [7]–[9].

[1]See ''Social media apps overwhelmingly dominate mobile traffic'', Business Insider, 2016: http://www.businessinsider.com/social-media-apps-overwhelmingly-dominate-mobile-traffic-2016-6?r=US&IR=T&IR=T

The number of applications brought about by MSNs is large and spans from bandwidth-hungry video sharing [10] through gaming [11], and to business-related proximity-based advertising [12]. Hence, modern MSNs are actively developing to cater for the trade-off between the high data rate and the low delay based on the actual application requirements [13]. However, the transferred data needs to be made secure independently of the usage scenario. Therefore, security and privacy issues in MSN environments have been articulated in recent years.

In particular, the authors in [14] provide a comprehensive survey on the existing MSN security mechanisms and methods. In doing so, they also conduct an evaluation of these in terms of their flexibility, operator protection, user anonymity, and independence of the actual service provider. Also, a new MSN architecture with appropriately communicating entities and their respective communication patterns has been proposed in [15]. In that work, the authors explored security and privacy requirements by focusing on social relationships among the users.

However, while these works offer valuable results on the requirements in terms of privacy and security, they do not address robustness of the proposed solutions against the malicious attacks that aim to extract sensitive information from the user devices, which becomes the main goal of this paper. In fact, ongoing proliferation of social applications where users store and communicate sensitive information, such as their bank account or credit card number, raises important concerns on the types of dedicated attacks and the ways to protect from them.

For instance, information leaks caused by emissions from electronic devices have been subject to many studies since 1985. Back then, content displayed on a monitor was reconstructed based on its electromagnetic emanation [16]. Further, that work was partially resumed in 2004 by [17], which utilized similar techniques to reconstruct the displayed content from the cable emissions. Later in 2006, acoustic emanations of keyboards were exploited to reveal the keys pressed by the users [18], [19].

Despite the fact that multiple works are targeting to protect from this type of attacks, which are still accumulating [20], contemporary mobile devices remain at high risk. Indeed, modern hand-held user equipment is increasingly vulnerable due to a multitude of supported applications.[2] Furthermore, since cloud-based and automated services become more common, smartphones can act as ''relays'' of critical information as they help manage multiple other systems [21].

In our daily applications, the operation of the underlying cryptographic algorithms – whether implemented in software or in hardware – is strongly affected by the immediate environment. Here, physical and social interactions can, in principle, be monitored by the malicious users, whereas the eavesdropped data itself may be employed in the subsequent cryptanalysis to extract sensitive and private information. Such data ''sniffed'' by the attackers is referred to as *side-channel information* and the corresponding actions that target to extract side-channel information are named *side-channel attacks* (SCAs).

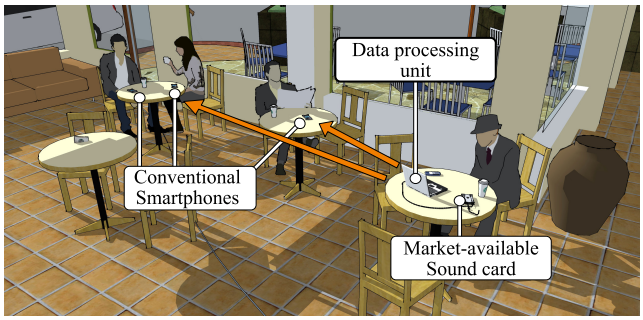

FIGURE 1. SCA execution example in a cafe environment (over the audio channel).

The key principle behind SCAs is to analyze how the specific cryptographic algorithm is implemented, rather than to disrupt the algorithm's operation. The SCAs are becoming increasingly widespread,[3] primarily due to the rapid proliferation of online services and platforms that are easily accessible trough user-owned smartphones (e.g., Amazon, Netflix, Spotify, etc.).

Today, one of the most dominant factors in executing SCAs is tightly connected to the vision, where smartphone is regarded as part of the Internet of Things ecosystem.[4] Accordingly, a variety of services associated with managing other devices are considered, such as processing status messages and making crucial decisions [22]. Indeed, taking into account improved connectivity offered by the MSNs on both social and network planes, attackers may be primarily interested in capturing the authorization data to then hijack access to private devices [23], see Fig. 1 for an example.

More technically, power consumers as part of the modern device electronics [24] operate simultaneously with the software applications and may thus create difficulties in registering the emanation (*traces*). To this end, analytical tools including machine learning techniques and signal processing [25], [26] may be utilized by the attackers to capture and analyze the electromagnetic radiation.

Against the above background, the aim of this work is to provide a comprehensive example of a possible SCA along the lines of extracting sensitive information from a smartphone by utilizing off-the-shelf, inexpensive equipment available to anybody. In doing so, we focus on decentralized MSNs due to their more dynamic behavior from the connectivity perspective [27]. In particular, our scenario of interest is

[2]See ''Choosing a Business Phone System: 2016 Buyer's Guide'', Business News Daily: http://www.businessnewsdaily.com/7149-business-phone-system-guide.html

[3]See ''Researchers show how side-channel attacks can be used to steal encryption keys on Amazon's cloud server'', PHYS Magazine, 2016: http://phys.org/news/2015-10-side-channel-encryption-keys-amazon-cloud.html

[4]See ''Is a smart phone an Internet of Things device?'', Mischa Dohler https://www.futurelearn.com/courses/internet-of-things/0/steps/8432

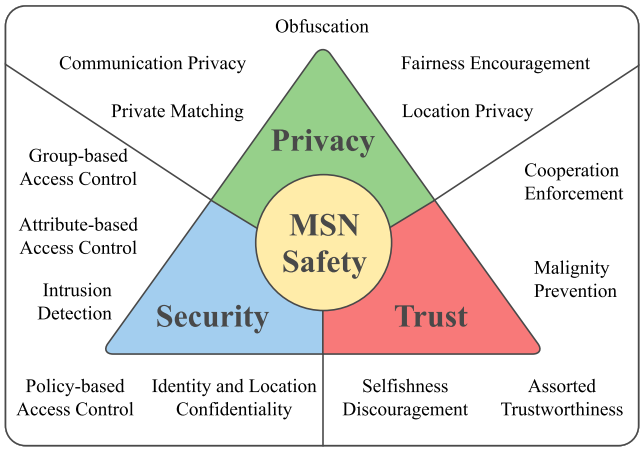

FIGURE 2. Security challenges in MSNs.

when a group of users belonging to a particular MSN exploit their social relationships to share data over the proximity-based links (i.e., on D2D communication channels) [28], [29]. This poses security challenges due to repetitive connection (re-)establishments, which in turn requires higher levels of security. Finally, we deliver an overview of possible enhanced attacks that are reviewed in conjunction with solutions that may be useful to avoid losing personal and sensitive information, which is kept within the smartphones and other personal user devices.

The following section discusses the security challenges in decentralized MSNs that need to be resolved.

II. SECURITY CHALLENGES IN DECENTRALIZED MSNs

This section brings attention to the main security issues pertaining to the *distributed MSNs* as well as discusses their ability to protect against a variety of attacks, failures, errors, and other unwanted situations [15]. Broadly, we may subdivide the key threats into the following categories: (i) trust, (ii) privacy, and (iii) security (see Fig. 2).

A. TRUST IN MSNs

The first critical consideration is related to the user's willingness to rely on actions performed by others in decentralized peer-to-peer (P2P) MSN environments, thus leading to the problems of *trust* [30]. In conventional infrastructure-based networks, reputation is maintained by the trusted authority, which significantly simplifies the routing and connectivity aspects between mobile nodes (both classical [31], [32] and virtualized [33]).

With respect to maintaining trust in P2P networks, a number of widely distributed protocols could be utilized to provide dynamic trust updates and offer efficient connectivity management [34]. In fact, it might be convenient to resolve the trust association challenges in conjunction with the direct connection establishment [35]. Despite the fact that a large number of techniques and solutions were introduced to support trustworthiness in MSNs [36]–[39], most developers still prefer relying on network assistance techniques to maintain the collective trustworthiness [6], [40].

To date, several well-known trust-related threats are: (i) Black Hole attack [41] is of the denial of service type. In case of its execution, a malicious trusted node is triggering an additional route discovery process for each connected user. Further, (ii) Sybil-attacks [42] target to create a large number of malicious identities in order to affect the levels of trust within a network. Finally, (iii) Node selfishness [43] is of concern i.e., when intermediate nodes are not willing to cooperate in the opportunistic manner but only consume the network resources.

To this end, managing reputation in large-scale distributed systems can be problematic and thus new solutions need to be developed considering energy and computational limitations of modern mobile devices. The MSN properties should also be accounted for in order to achieve better performance, which still remains a significant social challenge [44].

B. PRIVACY IN MSNs

Another category of threats is related to *privacy*, that is, the linkage of sensitive user information (such as identifiers, personal contacts, location-related data, etc.) [45]. Generally, user profiles in the MSN that contain the aforementioned data could be exploited to track the object's behavior [46]. In turn, privacy issues can be classified into two main groups: communications and location privacy.

Communications privacy reflects conventional approaches in privacy-centric network technologies. The tools utilized for reaching individual privacy are well-known and do not require an extensive introduction. Some examples in the following include authentication, non-repudiation, and cryptography, among others [47].

Modern MSN services support a wide range of location-based applications, such as proximity-based advertisements and photo sharing. At the same time, their users need to provide position information in order to gain access to the service that potentially causes privacy leakages. Adequate implementation of the location privacy management allows to prevent from the disclosure of sensitive user data. Many solutions are already developed to satisfy the requirements of this kind, such as [48], [49]: pseudo-anonymity, location obfuscation, key anonymity, etc.

Unfortunately, many users ignore the privacy-centric recommendations issued by the application developers and thus face the risks on a daily basis [50].

C. SECURITY IN MSNs

Finally, the remaining group of concerns in MSNs is related to protecting personal user data or other sensitive information during its transfer between the networked nodes [51]. In these situations, *security* needs to be maintained to protect users against the known attacks on ciphers [52] as well as to combat possible malicious behavior in the network [47]. Conventionally, the goals here are to ensure availability, authentication, confidentiality, and integrity of data altogether [53].

On the one hand, users have to be made aware that their behavior has a strong impact on the security procedures

within the MSN, while on the other hand there is a need for new methods and techniques that are capable of providing tight integration between privacy, trust, and security [54]. Hence, to help application developers offer increasingly security-centric solutions, one needs to develop measures that protect from the malicious subjects, who may perform SCAs to gain access to personal user data. This topic is discussed in detail in the remainder of this paper. Indeed, current security algorithms may not be sufficient to accommodate the rapidly growing variety of MSN services, where users make online payments, share their private data, while often relying on insecure links when engaging into direct communications [55].

FIGURE 3. The SCA prototype installation.

III. SCAs ON MOBILE USER DEVICES

In this section, the authors describe the target scenario and offer a decomposition of the applicable SCA. Clearly, by utilizing more complex and, consequently, expensive attack equipment, it is becoming easier to succeed with the SCA implementation. However, relying on the assumption that an attacker can only take advantage of inexpensive eavesdropping equipment, we conduct an example *affordable* SCA to obtain the user traces from a smartphone with a market-available external sound card. Our simple SCA prototype installation is represented in Fig. 3.

Due to a high number of constraints related to the SCAs, a dedicated application has been developed thus effectively serving as a ''sandbox'' for the respective cryptographic primitives (see Fig. 4). In this work, we aim to minimize the necessary user input operations as well as to provide with an easily extensible set of cryptographic primitives in conjunction with a controllable set of secret encryption keys. In addition, our considered application allows to perform the required cryptographic operations at high frequency for the rapid accumulation of sufficient data to carry out further attacks. The complete list of features in our developed ''sandbox'' application is given in Table 1.

Generally, the attack model could be represented in the following three steps:

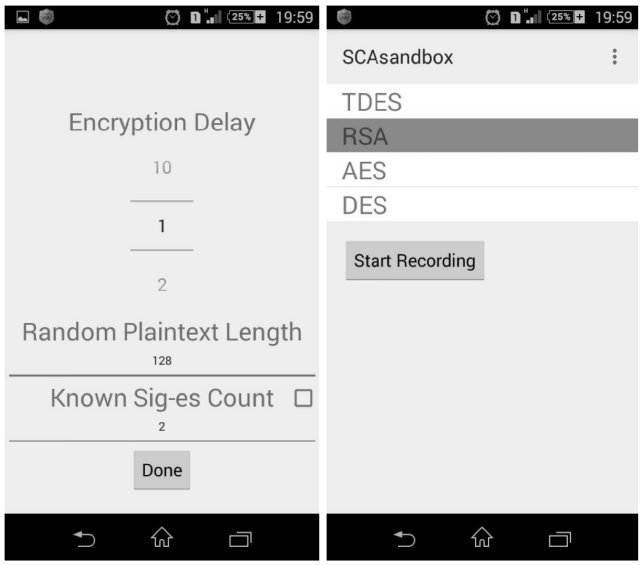

FIGURE 4. Custom ''sandbox'' Android application.

TABLE 1. The list of ''sandbox'' application features.

Supported feature
1) 3DES, AES, RSA, and DES encryption.
2) Controllable list of secret keys and initial vectors.
3) Support of time-stamps and detailed logging as it is important to maintain synchronization between the data and the attacking tool.
4) High frequency of cryptographic operations with controllable delay.
5) Generation of random plaintexts and keys.
6) Both Cipher Block Chaining (CBC) and Electronic Code Book (ECB) encryption.
7) Configurable number of equal starting signatures.

1) *Initial training*: The training is a process executed multiple times, thus making the deciphering more probable.
2) *Data collection*: The attacker's equipment is passively monitoring the target mobile phone location.
3) *Attack execution*: The data acquired in the training phase is utilized to decipher the actual information based on the real dataset from the data collection phase. This step could be integrated with the collection phase and executed dynamically on the go; or it can be a standalone execution run in a static manner after the data collection is complete.

At the initial training phase, it is feasible to generate several equal cryptographic operations (with the same plaintext and key material) before processing random plaintexts and/or keys. Here, the goal is to ensure synchronization between the attacking tool and the data in a manner as precise as possible. To this effect, if there are several equal signatures available within a trace, the detection of the encrypted data sequence of the starting and the ending points is more probable. This functionality may be applicable for noisy hardware inside the target device.

IV. DATA CAPTURE AND ANALYSIS

This section is focused on the useful data collection and its processing possibilities during the SCA. Based on the previously discussed assumptions, we utilize affordable and

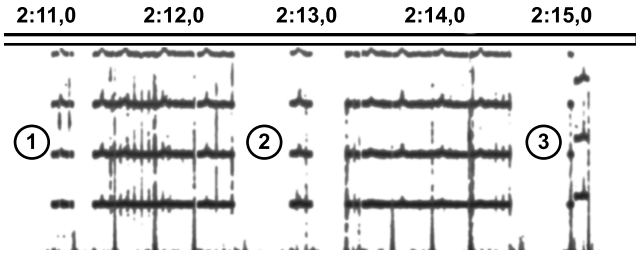

FIGURE 5. Example trace for Alcatel POP3: each encryption operation time is numbered.

market available equipment to execute the discussed SCA on a smart phone. We have selected two devices offered by different vendors in order to implement our SCA: Alcatel POP3 and Sony Xperia M2.

During the *initial training phase*, a *clean* run utilizing our ''sandbox'' application was executed. During this phase, most of the background activity of the target device was lowered to reduce the random behavior of the user. Conventionally, the cryptographic operation observations in the ''sandbox'' mode show relatively clearer traces, as it is depicted in Fig. 5. The capture presents an example of three cryptographic executions, which are numbered for clarity.

For example, the first one could be observed from point 2 : 11, 0 and up to 2 : 12, 5. Clearly, the second execution results in almost the same picture. It could be concluded that the operation in the ''sandbox'' mode is a meaningful way to fulfill the initial requirements of the training phase by completing a set of cryptographic fingerprints. When analyzing the traces after the training phase, we note a dramatic difference in the data definition – almost empty trace for Xperia M2. Apparently, the hardware-specific variations lead to completely different capture profiles. To this end, we decided to focus solely on the Alcatel POP3 analysis.

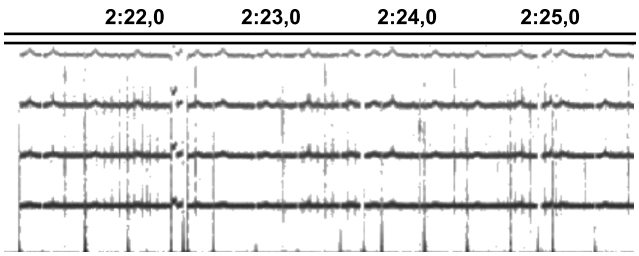

FIGURE 6. Example trace for Alcatel POP3: noisy traces during user interaction.

Fig. 6 demonstrates the results from Alcatel POP3 that satisfy the *data collection phase* requirements. The capture was performed by utilizing the same ''sandbox'' application, but running a number of side processes, such as enabling Wi-Fi, Bluetooth, and other modules. Random user input was examined as well. In particular, we see a totally undiagnosed noise flow for Alcatel (Fig. 6). It could be concluded that the SCA requires a significant effort during the initial training phase in order to achieve the acceptable accuracy.

The next step of our SCA is the raw data pre-processing for the subsequent neural network analysis. More specifically, the input data is converted into the vector format. Each vector contains the captured power record during a particular cryptographic operation. Next, the trace synchronization is achieved i.e., with the first N signatures of the trace vector, the attacker may predict the following signature by knowing the starting and ending points of the trace vector. The accuracy of this mechanism depends substantially on the sampling rate of the sound card as well as on the time periods required for executing the cryptographic operations on the device side.

Our custom-developed parser receives a trace recorded during the cryptographic operation generated by the ''sandbox'' application. The goal of the parser is to distinguish the cryptographic operations from the signal by removing the noise as well as to export them as separate vectors for further processing by the neural network. In our case, the parser comprises two distinct methods:

1) *Convolution function*: The parser considers the entire trace as well as the signatures as functions. The parser iterates through all the hypotheses regarding the first signature and calculates the resulting convolution function between a hypothesis and the entire trace. The peaks of the resulting functions indicate which hypotheses are the most probable and how many signatures matching every particular hypothesis are present in the trace, see Fig. 7. After the first signature has been identified, the parser continues through the trace detecting the starting and the ending points of other signatures. Finally, every signature is detected and saved as a separate vector.
2) *Convolution function within neighborhood*: The parser utilizes the set of time periods elapsed between the cryptographic operations as a ''lattice'' for the signature detection. A convolution function is calculated between every hypothesis of the first signature and the corresponding hypotheses of other detected signatures based on the execution times. To this end, it is assumed that the knowledge is available on the correct starting point of the first signature and the durations from the time stamp file. The parser determines which hypothesis regarding the first signature is the most appropriate based on the convolution analysis. The results achieved with this method are depicted in Fig. 8.

In conclusion, two interesting facts are observed after completing the pre-processing and parsing steps:

- Signatures are mostly not well-detailed due to the scarce sampling of the audio card. Hence, the level of detail has a tremendous impact on the captured data pre-processing.
- Some of the signatures may be detected incorrectly, as it is shown in Fig. 8. The detection error i.e., the chances of a wrong signature extraction caused by noise, is marked with a dashed line. A similar result was achieved by utilizing the first method on the same trace. The reason

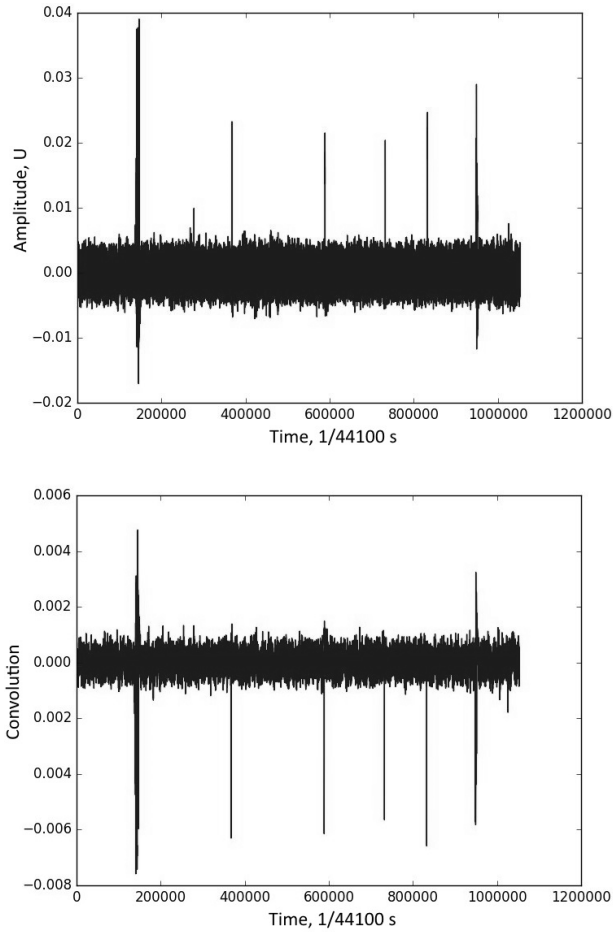

FIGURE 7. Detecting signatures with the first method.

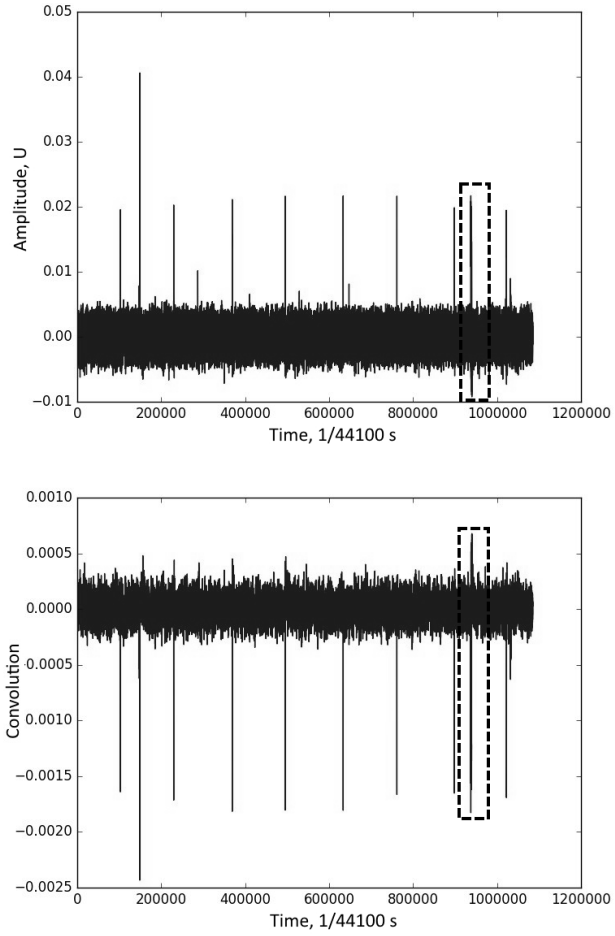

FIGURE 8. Detecting signatures with the second method.

for such an inaccuracy may be rooted in the low quality of the captured trace.

The utilization of more expensive and capable data capturing equipment is a solution to both of the above challenges.

V. ALTERNATIVE SCA APPROACHES

In this section, we elaborate on how the SCAs could be executed in non-straightforward ways as well as discuss the application of neural networks to the previously considered SCA.

As a result of the tests conducted in Section IV, we establish that performing a detailed analysis of traces by utilizing off-the-shelf sound card equipment is a complex task. This is mainly due to a significant difference between the sampling rates of the attacker device (i.e., 44100 Hz) and those of the encrypting devices (i.e., 6 MHz). Indeed, multiple details could be lost due to scarce sampling of the sound card, where only every 44100-th point of the original signal is available for the analysis. We may therefore conclude that for our case study the resolution of the obtained traces is rather low, meaning that only a small portion of potentially useful information on the sensitive data may be recovered.

Importantly, even with the inexpensive attacking equipment utilized in our tests, it remains possible to extract a portion of sensitive information from the user devices [56]. Apparently, by utilizing more powerful sound cards with higher sampling rates, it would be easier to eavesdrop for information on the user equipment, which threatens the safety of personal and sensitive data. In the following, we offer a description of improved methods that may be adopted to successfully extract information from a personal device together with some preventative measures that could be carried out by the users to avoid such attacks.

The key idea behind the discussed approach is to conduct an analysis of the parasitic signal based on the artificial neural network. This approach may not necessarily imply an absolute identification of a device's secret key, but brings an opportunity to determine the most probable states for each of its bits. Overall, the model of the attacking system consists of several functional modules, which are displayed in Fig. 9. The said model is based on an iterative approach and allows to optimize the attacking process.

In the first stage, it is crucial to validate as to whether the obtained traces are key- and plaintext-dependent. Multilayer perception is one of the possible solutions for this task [57]. In case a dependence exists, it becomes feasible to distinguish two keys, which differ from each

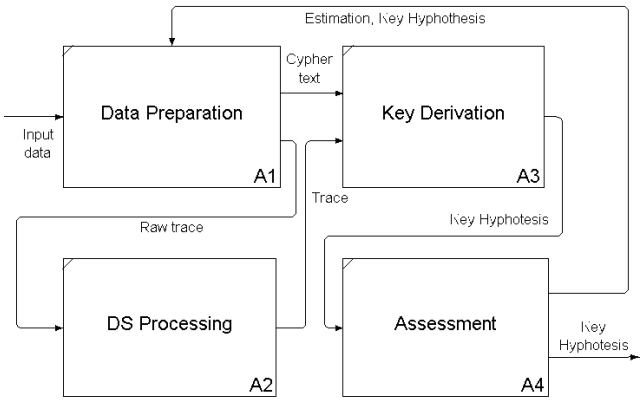

FIGURE 9. Functional model of the attack system.

other by only one particular bit. The following stage utilizes convolutional neural network (CNN) techniques with the corresponding matrices/weights [58], thus allowing to compute the so-called ''feature maps'' in order to distinguish each bit of the key [59].

Typically, each neuron at the output provides an estimation of the probability together with a response that indicates whether the input data is consistent with a particular class or not. One of the advantages of the proposed approach is to couple the probability and the value of each bit at the output. It allows to utilize various indicators for the error estimation as well as assess the confidence of the results. Indeed, error vectors could be represented either by a precise difference or by comparing a binary hypothesis with the actual key.

Further, the attack system has to differentiate between the three types of hypothesis estimations for configuring the exit conditions. The most harmful error that needs to be completely eliminated is the *confident-wrong hypothesis* on a particular bit. In case of this error, we have an incorrect result and cannot localize the position of the error. In contrast, if we have a limited number of *unconfidently-defined bits*, it is possible to ''flip'' each of them from zero to one and vice versa. Then, these several bits of the key could be derived by brute force. In case of *uncertainty*, it does not matter whether the hypothesis is correct or not i.e., in both cases the overall result would contain uncertain relevant bit and two probable keys required to be validated. Hence, each uncertain bit doubles the number of probable keys and thus the number of such errors has to be limited.

During the initial learning phase, error vectors are utilized for estimating the relevance of the data input. After the first stage, all of the input data have the corresponding associated weights that are further involved into the data preparation algorithm. In addition to input data, the correlation (i.e., XOR) between these and the actual key (i.e., the hypothesis of the key in case of a real attack) is evaluated. Thus produced correlation vectors may be utilized for optimization at the stage of the data preparation. Further, the part of the confidently defined key bits in the hypothesis may also be considered. In particular, the system selects the most applicable vector of the correlation to select the set of compliant input vectors. From this set, the vector with the highest weight is selected for this iteration as the input data.

There is a number of other reasons for selecting CNN as the main tool for the key derivation task. First, particular bits of the key have an impact only on the specific parts of the trace, which could be taken into account by the CNN i.e., there is a lower number of configurable links as compared to the multilayer perception [60]. Second, convolution computations can be performed by applying a higher number of streams in a simpler way than for most networks of other topologies. Finally, deep machine learning can examine much more complex correlations [61].

The disadvantage of using neural networks as a tool for our analysis is in their low efficiency for processing data that contain a large number of features. With regards to the parasitic signal, an attacker is not able to independently distinguish important features of each trace. To mitigate this ''curse of dimensionality'', we may utilize the normalized inter-class variance (NICV) method [62] allowing to identify the most vulnerable features of traces based on data classification and detection of anomalous dispersion deviations.

VI. POSSIBLE PROTECTION AGAINST SCAs

In the remainder of this text, we overview the main types of attacks, countermeasures, and guidelines that both the application developers and the end users may follow in order to increase their chances to protect from the SCAs. Even though some of these recommendations may seem straightforward and self-evident, we note that the majority of users and developers seldom comply with these guidelines and warnings.

A. SCAs CLASSIFICATION AND COUNTERMEASURES

In this work, the focus was set on the analysis employing a market-available sound card, which constitutes a particular case of the *power analysis* attack. However, it is important to emphasize that a number of other attacks may be implemented in the MSN as well. We thus briefly study the countermeasures against most types of the applicable SCAs.

1) POWER ANALYSIS

The attacker is analyzing the power consumption level of the devices by focusing on the modules operating with calculation of crypto primitives. The main requirement for this attack to be executed is close proximity.

Countermeasures: The main technique to avoid or mitigate the power analysis SCA is by introducing a tamper resistant body from the hardware point of view [63]. If such a straightforward solution is unacceptable, software developers may apply other techniques, including: (i) power randomization i.e., adding pseudo-random noise to the power consumption [64], (ii) data masking i.e., adding a data processing power figure uncorrelated with the secret [65], and (ii) data hiding i.e., concealing the intermediate encryption-related values in other activities [66].

2) TRAFFIC ANALYSIS

The attacker is analyzing the data flows that travel through the MSN to detect the critical node (e.g., a more trusted device) [67]. By detecting and compromising this node, the attacker may obtain higher influence on the MSN operation in general.

Countermeasures: One of the possible solutions is to camouflage the traffic i.e., anonymize the traffic of the critical node. It could be achieved by forcing the surrounding nodes to execute additional operations.

3) TIMING ATTACKS

This type of SCAs is targeted to exploit the time fluctuations during the secret-driven information process [68]. It may be conducted by utilizing the predefined look-up tables, early loop exiting, etc.

Countermeasures: One of the ways to avoid this type of attacks is to modify the intermediate values [69] or to add constant execution times [70]. Note that the discussed solutions may not be directly applicable for resource-constrained devices due to their high computation overheads. Other approaches known from the literature are to avoid the comparison of the secret information in a byte-by-byte manner as well as to utilize the look-up tables indexed with the secret information [71].

4) FAULT ANALYSIS

With this type of an active threat, the attacker attempts to make a fault induction to the node's input [72].

Countermeasures: Software developers should pay extreme attention to the input validation while developing applications that operate with sensitive data [73].

5) OTHER ATTACKS

Further, we list some of the SCAs that are not applicable for MSNs in particular, but should be taken into consideration generally.

Acoustic Cryptanalysis: The main difference with the power analysis attack is that the acoustic emissions can be obtained from the user input, such as e.g., keyboards [19]. There are no reliable ways to avoid this type of the SCA.

Thermal Imaging: This SCA is similar to the acoustic type, with the main difference that the analysis of a thermal figure from the CPU instead of the acoustic data [74] is exploited. A possible countermeasure is to utilize additional shield on the device. This, however, may bring along the overheating issues.

Visual Attack: One of the most direct attacks is ''spying'' i.e., capturing the light emissions from a display, led, or other device. Any signaling or sensitive information should thus be removed from the visual representation.

B. RECOMMENDATIONS FOR USERS

Conventionally, users do not have meaningful access to and explicit understanding of how software and hardware related to cryptography operate. For this reason, the first line of defense for the users against the malicious attackers is naturally to apply all the software updates on the operating system as well as the anti-virus software provided by the developers. In addition, it is highly recommended to pay particular attention to the devices coupled with the ''life-gateway'', that is, the smartphone [75]. In addition, a good practice is to use peripheral devices (power banks, external speakers, etc.) only developed by trusted manufacturers.[5]

Finally, any insecure long- and short-range wireless links (IEEE 802.11, Bluetooth, etc.) coupled with the malicious hardware[6] become a potential informational security threat [76], [77]. In such a case, enforcing all of the necessary software updates on a regular basis appears to be the most straightforward and comprehensive solution to keep the personal user devices safe from the SCAs.

VII. CONCLUSION

The explosive growth of new mobile-friendly applications and services is beginning to pose serious challenges to information security in mobile devices. In addition, proliferation of such services within the mobile social networks increases the chances for the user to be compromised and for a malicious attack to succeed. The aim of our research in this paper is to demonstrate that using low-cost off-the-shelf equipment for side-channel attacks on the smartphones is a serious threat, whereas such an intrusion remains hard to detect. In particular, our results reveal that even with low-end equipment the attackers are able to detect signals of the crypto computations. In fact, as shown in the latter part of this paper, with only a minor advancement in the attack tools it is possible to acquire even more informative traces.

Therefore, successful analysis of sensitive user data represents a serious threat for the personal user information stored inside a handheld device that is connected through online services. For this reason, after illustrating a possible more efficient attack that may be conducted to collect the information traces from other devices, we offer some guidelines that users may follow to decrease the levels of risk for their personal devices. As our future work, a possible extension here could be to increase the cost of the attack equipment (while still residing within the common consumer segment), both on the hardware and software sides, for recovering the secret stored in the mobile phones. In addition, the employed algorithms for parsing and classifying the traces could be improved further to leverage the extracted information even more efficiently.

[5]See ''Great. Now Even Your Headphones Can Spy on You'', WIRED, 2016: https://www.wired.com/2016/11/great-now-even-headphones-can-spy/

[6]See ''NSA's Own Hardware Backdoors May Still Be a Problem from Hell'', MIT Technology Review, 2013'': https://www.technologyreview.com/s/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/

REFERENCES

[1] L. Lin, L. Xu, S. Zhou, and Y. Xiang, "Trustworthiness-hypercube-based reliable communication in mobile social networks," *Inf. Sci.*, vol. 369, pp. 34–50, Nov. 2016.

[2] X. Hu, T. H. S. Chu, V. C. M. Leung, E. C. H. Ngai, P. Kruchten, and H. C. B. Chan, "A survey on mobile social networks: Applications, platforms, system architectures, and future research directions," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 3, pp. 1557–1581, 3rd Quart., 2015.

[3] Z. Su, Q. Xu, and Q. Qi, "Big data in mobile social networks: A QoE-oriented framework," *IEEE Netw.*, vol. 30, no. 1, pp. 52–57, Jan./Feb. 2016.

[4] D. Zhang, D. Zhang, H. Xiong, C.-H. Hsu, and A. V. Vasilakos, "BASA: Building mobile ad-hoc social networks on top of Android," *IEEE Netw.*, vol. 28, no. 1, pp. 4–9, Jan./Feb. 2014.

[5] E. Miluzzo *et al.*, "Sensing meets mobile social networks: The design, implementation and evaluation of the CenceMe application," in *Proc. 6th ACM Conf. Embedded Netw. Sensor Syst.*, Nov. 2008, pp. 337–350.

[6] N. Kayastha, D. Niyato, P. Wang, and E. Hossain, "Applications, architectures, and protocol design issues for mobile social networks: A survey," *Proc. IEEE*, vol. 99, no. 12, pp. 2130–2158, Dec. 2011.

[7] B. Bai, L. Wang, Z. Han, W. Chen, and T. Svensson, "Caching based socially-aware D2D communications in wireless content delivery networks: A hypergraph framework," *IEEE Wireless Commun.*, vol. 23, no. 4, pp. 74–81, Aug. 2016.

[8] N. Vastardis and K. Yang, "Mobile social networks: Architectures, social properties, and key research challenges," *IEEE Commun. Surv. Tuts.*, vol. 15, no. 3, pp. 1355–1371, 3rd Quart., 2013.

[9] Y. Li, S. Su, and S. Chen, "Social-aware resource allocation for device-to-device communications underlaying cellular networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 3, pp. 293–296, Jun. 2015.

[10] L. Gou *et al.*, "MobiSNA: A mobile video social network application," in *Proc. 8th ACM Int. Workshop Data Eng. Wireless Mobile Access*, Jun. 2009, pp. 53–56.

[11] W. Cai, V. C. M. Leung, and M. Chen, "Next generation mobile cloud gaming," in *Proc. IEEE 7th Int. Symp. Service Oriented Syst. Eng. (SOSE)*, Mar. 2013, pp. 551–560.

[12] R. Terlutter and M. L. Capella, "The gamification of advertising: Analysis and research directions of in-game advertising, advergames, and advertising in social network games," *J. Advertising*, vol. 42, nos. 2–3, pp. 95–112, 2013.

[13] A. Mohaien, D. F. Kune, E. Y. Vasserman, M. Kim, and Y. Kim, "Secure encounter-based mobile social networks: Requirements, designs, and tradeoffs," *IEEE Trans. Dependable Secure Computing*, vol. 10, no. 6, pp. 380–393, Nov. 2013.

[14] R. Ajami, N. A. Qirim, and N. Ramadan, "Privacy issues in mobile social networks," *Procedia Comput. Sci.*, vol. 10, pp. 672–679, 2012. [Online]. Available: http://ac.els-cdn.com/S1877050912004437/1-s2.0-S1877050912004437-main.pdf?_tid=bf598188-ff36-11e6-87db-00000aacb362&acdnat=1488452308_739a06060ff15c60d4e2369503ed39d6

[15] X. Liang, K. Zhang, X. Shen, and X. Lin, "Security and privacy in mobile social networks: Challenges and solutions," *IEEE Wireless Commun.*, vol. 21, no. 1, pp. 33–41, Feb. 2014.

[16] W. van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Comput. Secur.*, vol. 4, no. 4, pp. 269–286, Dec. 1985.

[17] M. G. Kuhn, "Electromagnetic eavesdropping risks of flat-panel displays," in *Proc. Int. Workshop Privacy Enhancing Technol.*, 2004, pp. 88–107.

[18] Y. Berger, A. Wool, and A. Yeredor, "Dictionary attacks using keyboard acoustic emanations," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, Oct. 2006, pp. 245–254.

[19] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 1, Oct. 2009, Art. no. 3.

[20] A. B. Levina and S. V. Taranov, "Construction of linear and robust codes that is based on the scaling function coefficients of wavelet transforms," *J. Appl. Ind. Math.*, vol. 9, no. 4, pp. 540–546, Oct. 2015.

[21] L. Militano, A. Orsino, G. Araniti, A. Molinaro, and A. Iera, "Overlapping coalitions for D2D-supported data uploading in LTE-A systems," in *Proc. IEEE 26th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Aug. 2015, pp. 1526–1530.

[22] J. Hosek, P. Masek, D. Kovac, M. Ries, and F. Kröpfl, "IP home gateway as universal multi-purpose enabler for smart home services," *Elektrotech. Informationstech.*, vol. 131, no. 4, pp. 123–128, Jul. 2014.

[23] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: Threats and challenges," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742, Dec. 2014.

[24] A. Pyattaev, K. Johnsson, S. Andreev, and Y. Koucheryavy, "Communication challenges in high-density deployments of wearable wireless devices," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 12–18, Feb. 2015.

[25] A. J. Maren, C. T. Harston, and R. M. Pap, *Handbook of Neural Computing Applications*. San Diego, CA, USA: Academic, 2014.

[26] M. Gholami, N. Cai, and R. W. Brennan, "An artificial neural network approach to the problem of wireless sensors network localization," *Robot. Comput.-Integr. Manuf.*, vol. 29, no. 1, pp. 96–109, Feb. 2013.

[27] Z. Su, Q. Xu, H. Zhu, and Y. Wang, "A novel design for content delivery over software defined mobile social networks," *IEEE Netw.*, vol. 29, no. 4, pp. 62–67, Jul./Aug. 2015.

[28] L. Wang, G. Araniti, C. Cao, W. Wang, and Y. Liu, "Device-to-device users clustering based on physical and social characteristics," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, p. 1, 2015.

[29] Z. Wu, L. Wang, G. Araniti, and Z. Han, "Exploiting social-interest interactions on user clustering and content dissemination in device-to-device communications," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Nov. 2015, pp. 1–6.

[30] F. E. Walter, S. Battiston, and F. Schweitzer, "A model of a trust-based recommendation system on a social network," *Auto. Agents Multi-Agent Syst.*, vol. 16, no. 1, pp. 57–74, Feb. 2008.

[31] K. Zhang, X. Liang, X. Shen, and R. Lu, "Exploiting multimedia services in mobile social networks from security and privacy perspectives," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 58–65, Mar. 2014.

[32] E. Bulut and B. K. Szymanski, "Exploiting friendship relations for efficient routing in mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 12, pp. 2254–2265, Dec. 2012.

[33] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Athanasios, "Software-defined and virtualized future mobile and wireless networks: A survey," *Mobile Netw. Appl.*, vol. 20, no. 1, pp. 4–18, Feb. 2014.

[34] H. Mousa, S. B. Mokhtar, O. Hasan, O. Younes, M. Hadhoud, and L. Brunie, "Trust management and reputation systems in mobile participatory sensing applications: A survey," *Comput. Netw.*, vol. 90, pp. 49–73, Oct. 2015.

[35] X. Wang, M. Chen, Z. Han, D. O. Wu, and T. T. Kwon, "TOSS: Traffic offloading by social network service-based opportunistic sharing in mobile social networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2014, pp. 2346–2354.

[36] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Comput. Human Behavior*, vol. 25, no. 1, pp. 153–160, Jan. 2009.

[37] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," *Ad Hoc Netw.*, vol. 11, no. 4, pp. 1497–1509, Jun. 2013.

[38] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

[39] J. Li, Z. Zhang, and W. Zhang, "MobiTrust: Trust management system in mobile social computing," in *Proc. IEEE 10th Int. Conf. Comput. Inf. Technol. (CIT)*, Jun. 2010, pp. 954–959.

[40] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Social trust and social reciprocity based cooperative D2D communications," in *Proc. 14th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Jul./Aug. 2013, pp. 187–196.

[41] S. Kumar and K. Dutta, "Intrusion detection technique for black hole attack in mobile ad hoc networks," *Int. J. Inf. Privacy, Secur. Integrity*, vol. 2, no. 2, pp. 81–101, 2015.

[42] G. Wang, F. Musau, S. Guo, and M. B. Abdullahi, "Neighbor similarity trust against sybil attack in P2P E-commerce," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 3, pp. 824–833, Mar. 2015.

[43] J. Ren, Y. Zhang, K. Zhang, and X. S. Shen, "SACRM: Social aware crowdsourcing with reputation management in mobile sensing," *Comput. Commun.*, vol. 65, pp. 55–65, Jul. 2015.

[44] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 5, pp. 1200–1210, May 2014.

[45] R. Zhang, J. Zhang, Y. Zhang, J. Sun, and G. Yan, "Privacy-preserving profile matching for proximity-based mobile social networking," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 656–668, Sep. 2013.

[46] M. Li, S. Yu, N. Cao, and W. Lou, "Privacy-preserving distributed profile matching in proximity-based mobile social networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2024–2033, May 2013.

[47] J. Zhou, Z. Cao, X. Dong, X. Lin, and A. V. Vasilakos, "Securing m-healthcare social networks: Challenges, countermeasures and future directions," *IEEE Wireless Commun.*, vol. 20, no. 4, pp. 12–21, Aug. 2013.

[48] M. Wernke, P. Skvortsov, and F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Pers. Ubiquitous Comput.*, vol. 18, no. 1, pp. 163–175, Jan. 2014.
[49] M. Srivatsa and M. Hicks, "Deanonymizing mobility traces: Using social network as a side-channel," in *Proc. ACM Conf. Comput. Commun. Secur.*, Oct. 2012, pp. 628–637.
[50] Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2010, pp. 1–9.
[51] D. D. Hwang *et al.*, "AES-based security coprocessor IC in 0.18-μm CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.
[52] B. Bilgin, A. Bogdanov, M. Kneevic, F. Mendel, and Q. Wang, "FIDES: Lightweight authenticated cipher with side-channel resistance for constrained hardware," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2013, pp. 142–158.
[53] X. Liang, X. Lin, and X. S. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 310–320, Feb. 2014.
[54] H. Li, H. Zhu, S. Du, X. Liang, and X. Shen, "Privacy leakage of location sharing in mobile social networks: Attacks and defense," *IEEE Trans. Depend. Sec. Comput.*, to be published. [Online]. Available: http://ieeexplore.ieee.org/document/7556276/
[55] T. Ning, Z. Yang, H. Wu, and Z. Han, "Self-interest-driven incentives for ad dissemination in autonomous mobile social networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2310–2318.
[56] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom, "ECDSA key extraction from mobile devices via nonintrusive physical side channels," *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 1626–1638.
[57] J. Tang, C. Deng, and G.-B. Huang, "Extreme learning machine for multilayer perceptron," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 4, pp. 809–821, Apr. 2016.
[58] J. Zbontar and Y. LeCun, "Stereo matching by training a convolutional neural network to compare image patches," *J. Mach. Learn. Res.*, vol. 17, pp. 1–32, Jan. 2016.
[59] W. Zhang, K.-W. Wong, H. Yu, and Z.-L. Zhu, "A symmetric color image encryption algorithm using the intrinsic features of bit distributions," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 3, pp. 584–600, Mar. 2013.
[60] D. W. Ruck, S. K. Rogers, M. Kabrisky, M. E. Oxley, and B. W. Suter, "The multilayer perceptron as an approximation to a Bayes optimal discriminant function," *IEEE Trans. Neural Netw.*, vol. 1, no. 4, pp. 296–298, Dec. 1990.
[61] L. Romaszko, "Signal correlation prediction using convolutional neural networks," in *Proc. JMLR, Workshop Conf.*, vol. 46. 2015, pp. 45–56.
[62] S. Bhasin, J.-L. Danger, S. Guilley, and Z. Najm, "NICV: Normalized inter-class variance for detection of side-channel leakage," in *Proc. Int. Symp. Electromagn. Compat., Tokyo (EMC/Tokyo)*, May 2014, pp. 310–313.
[63] M. Hassinen and K. Hyppönen, and E. Trichina, "Utilizing national public-key infrastructure in mobile payment systems," *Electron. Commerce Res. Appl.*, vol. 7, no. 2, pp. 214–231, 2008.
[64] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Proc. Annu. Int. Cryptol. Conf.*, 1999, pp. 398–412.
[65] E. Prouff and M. Rivain, "Masking against side-channel attacks: A formal security proof," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2013, pp. 142–159.
[66] T. Plos, M. Hutter, and M. Feldhofer, "Evaluation of side-channel preprocessing techniques on cryptographic-enabled HF and UHF RFID-tag prototypes," in *Proc. Workshop RFID Secur.*, 2008, pp. 114–127.
[67] F. Zhang *et al.*, "Thwarting Wi-Fi side-channel analysis through traffic demultiplexing," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 86–98, Jan. 2014.
[68] D. Genkin, L. Pachmanov, I. Pipman, A. Shamir, and E. Tromer, "Physical key extraction attacks on PCs," *ACM Commun.*, vol. 59, no. 6, pp. 70–79, Jun. 2016.
[69] R. Hund, C. Willems, and T. Holz, "Practical timing side channel attacks against kernel space ASLR," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2013, pp. 191–205.
[70] P. Hodgers, N. Hanley, and M. O'Neill, "Pre-processing power traces to defeat random clocking countermeasures," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2015, pp. 85–88.
[71] E. Tromer, D. A. Osvik, and A. Shamir, "Efficient cache attacks on AES, and countermeasures," *J. Cryptol.*, vol. 23, no. 1, pp. 37–71, 2010.
[72] Y. Li, M. Chen, and J. Wang, "Introduction to side-channel attacks and fault attacks," in *Proc. Asia–Pacific Int. Symp. Electromagn. Compat. (APEMC)*, vol. 1. May 2016, pp. 573–575.
[73] T. Scholte, W. Robertson, D. Balzarotti, and E. Kirda, "An empirical analysis of input validation mechanisms in Web applications and languages," in *Proc. 27th Annu. ACM Symp. Appl. Comput.*, Mar. 2012, pp. 1419–1426.
[74] P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz, "A pilot study on the security of pattern screen-lock methods and soft side channel attacks," in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Apr. 2013, pp. 1–6.
[75] L. Militano, M. Condoluci, G. Araniti, A. Molinaro, and A. Iera, "When D2D communication improves group oriented services in beyond 4G networks," *Wireless Netw.*, vol. 21, no. 4, pp. 1363–1377, May 2015.
[76] S. Sethumadhavan, A. Waksman, M. Suozzo, Y. Huang, and J. Eum, "Trustworthy hardware from untrusted components," *ACM Commun.*, vol. 58, no. 9, pp. 60–71, Sep. 2015.
[77] A. Waksman and S. Sethumadhavan, "Silencing hardware backdoors," in *Proc. IEEE Symp. Secur. Privacy*, May 2011, pp. 49–63.

ALEKSANDR OMETOV received the M.Sc. degree (Hons.) in telecommunications from the Department of Electronics and Communications Engineering, Tampere University of Technology (TUT), Finland, in 2016, and the Specialist degree in information security from the Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia, in 2013. He has been a Research Assistant with TUT since 2013. His major research interests are wireless communications, information security, heterogeneous networking, cooperative communications, and machine-to-machine applications.

ALLA LEVINA received the Specialist and Ph.D. degrees from the Department of Math, Saint Petersburg State University, Russia, in 2005 and 2009, respectively. She is currently an Associate Professor with the National Research University of Information Technologies, Mechanics and Optics, Department of Secure Information Technology, ITMO University, where she is Co-Head of SCA Research Laboratory. Her major research interests are side-channel attacks, information security, wavelet transforms, and coding theory.

PAVEL BORISENKO received the B.Sc. degree in information security from ITMO University, Saint Petersburg, Russia, in 2015, and the M.Sc. degree in information security from the SCA Research Laboratory, ITMO University, with the main focus on side-channel attacks. He is interested in side-channel attacks, machine learning, and vulnerabilities of mobile devices.

ROMAN MOSTOVOY received the Specialist degree in information security from the Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO), Saint Petersburg, Russia, in 2015. He is currently pursuing the Ph.D. degree with the SCA Research Laboratory, ITMO University. His major research interests are side-channel attacks, information security, security vulnerabilities, signal processing, and machine learning.

ANTONINO ORSINO received the B.Sc. degree in telecommunications engineering from the University Mediterranea of Reggio Calabria, Italy, in 2009, and the M.Sc. degree from the University of Padova, Italy, in 2012. He is currently pursuing the Ph.D. degree with DIIES Department, University Mediterranea of Reggio Calabria. He is currently a Research Assistant with the Department of Electronics and Communications Engineering, Tampere University of Technology, Finland. His current research interests include device-to-device and machine-to-machine communications in 4G/5G cellular systems, multicast, spectrum sharing, and Internet of Things.

SERGEY ANDREEV received the Specialist and Cand.Sc. degrees from the Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia, in 2006 and 2009, respectively, and the Ph.D. degree from the Tampere University of Technology in 2012. He is currently a Senior Research Scientist with the Department of Electronics and Communications Engineering, Tampere University of Technology, Finland. He has co-authored over 120 publications in his research fields. His research interests include wireless communications, energy efficiency, heterogeneous networking, cooperative communications, and machine-to-machine applications.