International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Mobile Social Networking below Side-Channel Attacks: sensible Security Challenges

Geetha Kurikala[1], K Gurnadha Gupta[2]

Computer Science and Engineering, Sri Indu College of Engineering & Technology, Telangana, India

ABSTRACT

Mobile social networks (MSNs) are the networks of people with similar interests connected to every alternative through their mobile devices. Recently, MSNs are proliferating quick supported by rising wireless technologies that permit achieving a lot of economical communication and higher networking performance across the key parameters, like lower delay, higher rate, and higher coverage. At a similar time, most of the MSN users don't absolutely acknowledge the importance of security on their hand-held mobile devices. Owing to this reality, multiple attacks aimed toward capturing personal info and sensitive user information become a growing concern, oil-fired by the avalanche of latest MSN applications and services. Therefore, the goal of this work is to know whether or not the up to date user instrumentality is prone to compromising its sensitive info to the attackers. As associate degree example, numerous info security algorithms enforced in trendy smart phones are therefore tested to try the extraction of the same personal information supported the traces registered with cheap up to date audio cards. Our obtained results indicate that the oftenest, that constitutes the strongest limitation of the off-the-rack side-channel attack instrumentality, solely delivers low-informative traces. However, the success probabilities to recover sensitive information keep on a mobile device could increase considerably once utilizing a lot of economical analytical techniques additionally as using a lot of complicated attack instrumentality. Finally, we elaborate on the possible utilization of neural networks to boost 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.

Keywords : 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 of had the infrastructure of a network operator, which is possible over a range of wireless technologies [1]. This made heterogeneous property fuels the novel networking paradigm, named mobile social networks (MSNs), wherever the property and information sharing patterns among users square measure supported their social contacts and relationships [2], [3]. According to Sand vine 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 in supporting the increasing user data rate requirements [4].

One of the remainder works that focus on MSNs from the angle of coupling the practicality of standard social networks with the options of mobile communications was summarized in [5]. In an exceedingly shell, the authors planned that the users could exploit their social contacts so as to boost the networking potency from a user-centric perspective. Another line of analysis on MSNs considers standard social networks with a centralized management unit, wherever the information is also no inheritable directly through mobile devices

just in case the central node fails [6]. In these things, the devices in proximity could communicate by utilizing short-range radio technologies (e.g., device-to-device communications D2D) [7] [9].

The number of applications caused by MSNs is giant and spans from bandwidth-hungry video sharing [10] through gambling [11], and to business-related proximity-based advertising [12]. Hence, trendy MSNs area unit actively developing to cater for the trade-off between the high rate and therefore the low delay supported the particular application necessities. However, the transferred knowledge has to be created secure severally of the usage situation. Therefore, security and privacy problems in MSN environments are articulated in recent years.

In explicit, the authors in give a comprehensive survey on the present MSN security mechanisms and ways. In doing therefore, they additionally conduct associate analysis of those in terms of their flexibility, operator protection, user obscurity, and independence of the particular service supplier. Also, a replacement MSN design with fitly act entities and their several communication patterns has been projected in. In this work, the authors explored security and privacy necessities by specializing in social relationships among the users.

However, whereas these works provide valuable results on the wants in terms of privacy and security, they are doing not address strength of the projected solutions against the malicious attacks that aim to extract sensitive info from the user devices that becomes the most goal of this paper. In fact, in progress proliferation of social applications wherever users store and communicate sensitive info, like their checking account or MasterCard variety, raises vital issues regarding the categories of dedicated attacks and therefore the ways that to protect from them.

For instance, info leaks caused by emissions from electronic devices are subject to several studies since 1985. Back then, content displayed on a monitor was reconstructed supported its magnetic attraction emanation [16]. Further, that job was part resumed in 2004 by [that used similar techniques to reconstruct the displayed content from the cable emissions. Later in 2006, acoustic emanations of keyboards were exploited to reveal the keys ironed by the users.

Despite the actual fact that multiple works area unit targeting to guar from this kind of attacks, that area unit still accumulating [20], modern mobile devices stay at high risk. Indeed, the fashionable hand-held user instrumentality is more and more vulnerable because of a mess of supported applications.2 what is more, since cloud-based and automatic services become a lot of common, smart phones will act as ``relays" of vital info as they assist manage multiple different systems .

In our daily applications, the operation of the underlying crypto logical algorithms whether or not enforced in package or in hardware is powerfully littered with the immediate surroundings. Here, physical and social interactions will, in theory, be monitored by the malicious users, whereas the eavesdropped knowledge itself is also used within the ulterior scientific discipline to extract sensitive and personal info. Such knowledge ``sniffed" by the attackers is cited as side-channel info and therefore the corresponding actions that focus on to extract side-channel info area unit named side-channel attacks (SCAs).

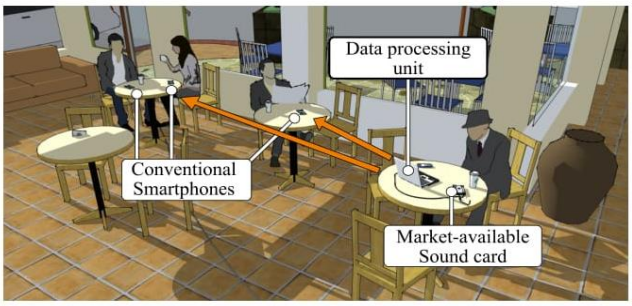

FIGURE 1. SCA execution example in a cafe environment (over the audio channel).

The key principle behind SCAs is to research however the precise crypto logical rule is enforced, instead of to disrupt the algorithm's operation. The SCAs are getting more and more widespread, 3 primarily because of the fast proliferation of on-line services and platforms that area unit simply accessible trough user-owned smart phones (e.g., Amazon, Net ix, spottily, etc.).

Today, one in every of the foremost dominant factors in execution SCAs is tightly connected to the vision, wherever Smartphone is considered a part of the web of Things system.4 consequently, a range of services related to managing different devices area unit thought-about, like process standing messages and creating crucial choices .Indeed, taking into consideration improved property offered by the MSNs on each social and network planes, attackers is also primarily

inquisitive about capturing the authorization knowledge to then hijack access to personal devices see Fig. one for associate example.

More technically, power customers as a part of the fashionable device physics operate at the same time with the package applications and should therefore produce difficulties in registering the emanation (traces). To the present finish, analytical tools together with machine learning techniques and signal processing are also used by the attackers to capture and analyze the radiation.

Against the higher than background, the aim of this work is to supply a comprehensive example of a potential SCA on the lines of extracting sensitive info from a Smartphone by utilizing off-the-peg, cheap instrumentality obtainable to anybody. In doing therefore, we tend to specialize in suburbanized MSNs because of their lot of dynamic behavior from the property perspective. Above all, our situation of interferes is once a gaggle of users happiness to a selected MSN exploit their social relationships to share knowledge over the proximity-based links (i.e., on D2D communication channels). This poses security challenges because of repetitive association (re-) establishments that successively need higher levels of security. Finally, we tend to deliver a summary of potential increased attacks that area unit reviewed in conjunction with solutions that will be helpful to avoid losing personal and sensitive info that is unbroken among the smart phones and different personal user devices.

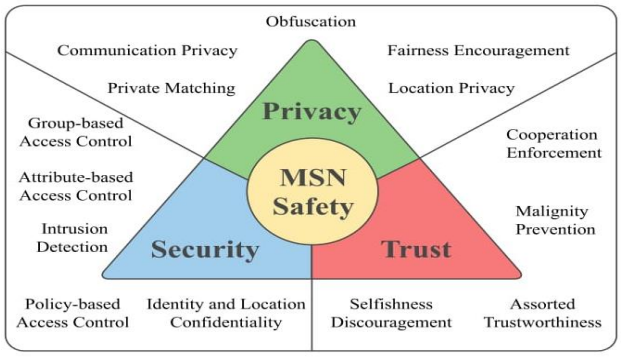

FIGURE 2. Security challenges in MSNs.

The following section discusses the safety challenges in suburbanized MSNs that require being resolved.

II. METHODS AND MATERIAL

1. Security Challenges IN Suburbanized MSNs

This section brings attention to the most security problems referring to the distributed MSNs furthermore as discusses their ability to guard against a range of attacks, failures, errors, and different unwanted things [15]. Broadly, we tend to could subdivide the key threats into the subsequent categories: (i) trust, (ii) privacy, and (iii) security (see Fig. 2).

A. TRUST IN MSNs

The first vital thought is said to the user's temperament to deem actions performed by others in suburbanized peer-to-peer (P2P) MSN environments, therefore resulting in the issues of trust [30]. In typical infrastructure-based networks, name is maintained by the sure authority that considerably samples the routing and property aspects between mobile nodes (both classical and virtualized])

To date, many well-known trust-related threats are :(i) Part attack is that the denial of service sort. Within the case of its execution, a malicious sure node is triggering a further route discovery method for every connected user. Further, (ii) Sybil-attacks target to form an outsized variety of malicious identities so as to have an effect on the degree of trust among a network. Finally, (iii) Node sell shyness is of concern i.e., once intermediate nodes aren't willing to join forces within the expedient manner however solely consuming the network resources.

To this finish, managing name in large-scale distributed systems are often problematic and therefore new solutions got to be developed considering energy and process limitations of contemporary mobile devices. The MSN properties ought to even be accounted for so as to attain higher performance that still remains a major social challenge.

B. PRIVACY IN MSNs

Another class of threats is said to privacy, that is, the linkage of sensitive user info (such as identifiers, personal contacts, location-related knowledge, etc.). Generally, user roles within the MSN that contain the aforesaid knowledge may be exploited to trace the object's behavior. In turn, privacy problems are often classified into 2 main groups: communications and placement privacy.

Communications privacy rejects typical approaches in privacy-centric network technologies. The tools used for reaching individual privacy area unit well-known and don't need an intensive introduction. Some samples of the subsequent embody authentication, non-repudiation, and cryptography, among others.
Modern MSN services support a large varies of location-based applications, like proximity-based advertisements and image sharing. At a similar time, their users got to give position info so as to achieve access to the service that doubtless causes privacy leakages. Adequate implementation of the situation privacy management permits preventing the revealing of sensitive user knowledge. Several solutions area unit already developed to satisfy the wants of this type, like pseudo-anonymity, location obfuscation, key obscurity, etc.

Unfortunately, several users ignore the privacy-centric recommendations issued by the applying developers and so face the risks on an each day.

C. SECURITY IN MSNs

Finally, the remaining cluster of considerations in MSNs is said to protective personal user knowledge or different sensitive info throughout its transfer between the networked nodes .In these things, security must be maintained to shield users against the acknowledged attacks on ciphers furthermore on combat doable malicious behavior within the network .Convention-ally, the goals here are to make sure handiness, authentication, con veniality, and integrity of knowledge altogether.

On the one hand, users need to be created aware that their behavior features a sturdy impact on the protection procedures Within the MSN, whereas on the opposite hand there's a desire for brand new ways and techniques that square measure capable of providing tight integration between privacy, trust, and security . Hence, to assist application developers supply more and more security-centric solutions, one must develop measures that shield from the malicious subjects, and UNi agency could perform SCAs to achieve access to non-public user knowledge. This subject is mentioned well within the remainder of this paper. Indeed, current security algorithms might not be sufficient to accommodate the chop-chop growing style of MSN services, wherever users create on-line payments, share their personal knowledge, whereas usually hoping on insecure links once participating into direct communications.

FIGURE 3. **The SCA prototype installation.**

2. SCAs On Mobile User Devices

In this section, the authors describe the target state of affairs and supply a decomposition of the applicable SCA. Clearly, by utilizing a lot of complicated and, consequently, pricy attack instrumentality, it's turning into easier to succeed with the SCA implementation. However, hoping on the idea that associate assailant will solely benefit of cheap eaves-dropping instrumentality, we tend to conduct associate example cheap SCA to get the user traces from a Smartphone with a market-available external sound card. Our straightforward SCA paradigm installation is delineating in Fig. 3.

Due to a high range of constraints associated with the SCAs, a passionate application has been developed so effectively serving as a ``sandbox" for the individual crypto logic primitives (see Fig. 4). During this work, we tend to aim to attenuate the required user input operations furthermore on offer with associate simply extensile set of crypto logic primitives in conjunction with a governable set of secret coding keys. Additionally, our thought of application permits to perform the desired crypto logic operations at high frequency for the speedy accumulation of sufficient knowledge to hold out further attacks. The entire list of options in our developed ``sandbox" application is given in Table one.

Generally, the attack model may well be delineating within the following 3 steps:

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.

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.

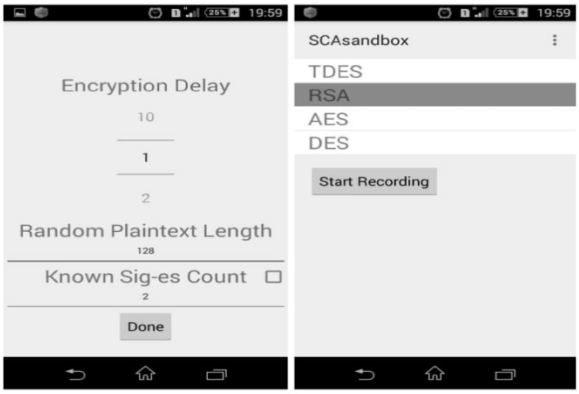

FIGURE 4. Custom "sandbox" Android application.

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.

At the initial training phase, it is feasible to generate several equal cryptographic operations (with the same

3. 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 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.

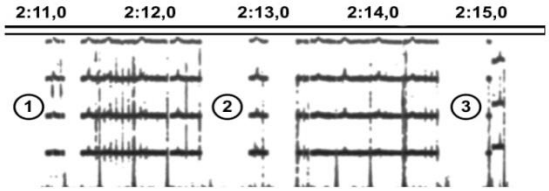

FIGURE 5. Example trace for Alcatel POP3: each encryption operation time is numbered.

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.

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 ``sand-box" 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 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 le. The parser determines which hypothesis regarding the first signature is the most appropriate based on the convolution analysis.

In conclusion, 2 attention-grabbing facts are ascertained when finishing the pre-processing and parsing steps:

Signatures are largely not well-detailed attributable to the scarce sampling of the audio card. Hence, the extent of detail features a tremendous impact on the captured knowledge reprocessing.
The detection error i.e., the probabilities of a wrong signature extraction caused by noise, is marked with a broken line. The same result was achieved by utilizing the civil time methodology on a similar trace. The reason for such associate quality could also be unmoving within the caliber of the captured trace.

III. RESULTS AND DISCUSSION

1. Various SCA APPROACHES

In this section, we have a tendency to elaborate on however the SCAs might be dead in non-straightforward ways in which in addition as discuss the appliance of neural networks to the antecedently thought of SCA.

As a results of the tests conducted in Section IV, we have a tendency to establish that activity an in depth analysis of traces by utilizing off-the-rack sound card instrumentation could be a complicated task. This is often in the main as a result of a significant distinction between the sampling rates of the aggressor device (i.e., 44100 Hz) and people of the encrypting devices (i.e., 6 MHz). Indeed, multiple details might be lost as a result of scarce sampling of the sound card, wherever solely each 44100-th purpose of the first signal is out there for the analysis. We have a tendency to could so conclude that for our case study the resolution of the obtained

traces is very low, which means that solely satiny low portion of probably helpful data on the sensitive knowledge could also be recovered. Importantly, even with the cheap assaultive equipment used in our tests, it remains potential to extract a little of sensitive data from the user devices. Apparently, by utilizing a lot of powerful sound cards with higher sampling rates, it might be easier to listen in for data on the user instrumentation that threatens the security of private and sensitive knowledge. Within the following, we provide an outline of improved strategies which will be adopted to with success extract data from a private device at the side of some preventative measures that might be car-ride out by the users to avoid such attacks.

The key plan behind the mentioned approach is to conduct Associate in nursing analysis of the parasitic signal supported the arterial neural network. This approach might not essentially imply Associate in Nursing absolute identify ion of a device's secret key, however brings a chance to work out the foremost probable states for every of its bits. Overall, the model of the assaultive system consists of many practical modules. The same model relies on Associate in nursing reiterative approach and permits to optimize the assaultive method.

In the first stage, it's crucial to validate on whether or not they obtained traces square measure key- and plaintext-dependent. Multilayer perception is one in every of the potential solutions for this task. Just in case dependence exists, it becomes possible to differentiate 2 keys that dissent from every other by just one explicit bit. The subsequent stage utilizes convolution neural network (CNN) techniques with the corresponding matrices/weights, so permitting to reason the questionable ``feature maps" so as to differentiate every little bit of the key.

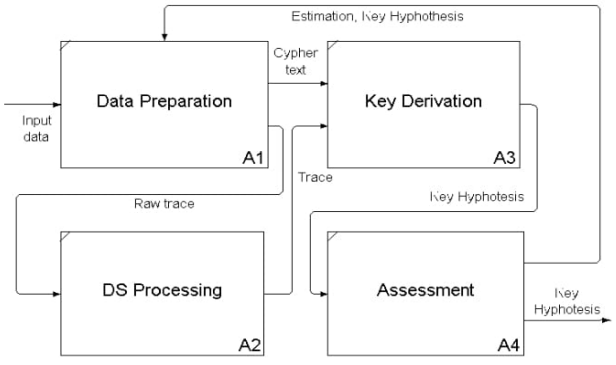

FIGURE 9. Functional model of the attack system.

Typically, every vegetative cell at the output provides Associate in Nursing estimation of the chance at the side of a response that indicates whether or not the computer file is according to a specific category or not. One in every of the benefits of the planned approach is to couple the chance and therefore the worth of every bit at the output. It permits to utilize numerous indicators for the error estimation in addition as assess the con dance of the results. Indeed, error vectors might be pictured either by a definite distinction or by comparison a binary hypothesis with the particular key. The disadvantage of victimization neural networks as a tool for our analysis is in their low efficiency for process knowledge that contains an oversized variety of options. With regards to the parasitic signal, Associate in nursing aggressor isn't ready to severally distinguish necessary options of every trace. To mitigate this ``curse of dimensionality", we have a tendency to could utilize the normalized inter-class variance (NICV) technique permitting to spot the foremost vulnerable options of traces supported knowledge classy ion and detection of abnormal dispersion deviations.

2. Potential PROTECTION AGAINST SCAs

In the remainder of this text, we have a tendency to summary the most sorts of attacks, countermeasures, and pointers that each the application developers and therefore the finish users could follow so as to extend their probabilities to guard from the SCAs. Although a number of these recommendations could seem simple and taken for granted, we have a tendency to note that the bulk of users and developers rarely adjust to these pointers and warnings.

A. SCAs Classification and Countermeasures

In this work, the main target was assailing the analysis using a market-available sound card that constitutes a specific case of the ability analysis attack. However, it's important to emphasize that variety of different attacks could also be enforced within the MSN in addition. We have a tendency to so cheese y study the countermeasures against most sorts of the applicable SCAs.

1) POWER ANALYSIS

The aggressor is analyzing the ability consumption level of the devices by specializing in the modules operational with calculation of crypto primitives. The most demand for this attack to be dead is shut proximity.

Countermeasures: the most technique to avoid or mitigate the ability analysis SCA is by introducing a tamper resistant body from the hardware purpose of read. If such a straight-forward answer is unacceptable, package developers could apply different techniques, including: (i) power organization i.e., adding pseudo-random noise to the ability consumption , (ii) knowledge masking i.e., adding a knowledge process power gore unrelated with the key , and (ii) knowledge concealing i.e., concealing the intermediate encryption-related values in different activities.

2) TRAFFIC ANALYSIS

The aggressor is analyzing the info owes that travel through the MSN to discover the important node (e.g., a lot of trusty device). By police work and compromising this node, the aggressor could acquire higher in hence on the MSN operation generally.

Countermeasures: one in every of the potential solutions is to commonage the tram c i.e., anonymizes the tram c of the important node. It might be achieved by forcing the encircling nodes to execute extra operations.

3) Temporal order ATTACKS

This type of SCAs is targeted to take advantage of the time actuations throughout the secret-driven data method. It's going to be conducted by utilizing the preened look-up tables, early loop exiting, etc.
Countermeasures: one in every of the ways in which to avoid this kind of attacks is to switch the intermediate values or to feature constant execution times. Note that the mentioned solutions might not be directly applicable for resource-constrained devices as a result of their high computation overheads. Different approaches far-famed from the literature square measure to avoid the comparison of the key data during a byte-by-byte manner in addition on utilizes the look-up tables indexed with the key data.

4) FAULT ANALYSIS

With this kind of a lively threat, the aggressor makes an attempt to create a fault induction to the node's input.
Countermeasures: package developers ought to pay extreme attention to the input validation whereas developing applications that operate with sensitive knowledge.

5) Different ATTACKS

Further, we have a tendency to list a number of the SCAs that aren't applicable for MSNs above all, however ought to be taken into thought usually.

Acoustic Cryptanalysis: the most distinction with the ability analysis attack is that the acoustic emissions may be obtained from the user input, such as e.g., keyboards. There are not any reliable ways in which to avoid this kind of the SCA.

Thermal Imaging: This SCA is comparable to the acoustic kind, with the most distinction that the analysis of a thermalgure from the C.P.U. rather than the acoustic knowledge is exploited. A potential step is to utilize extra defend on the device. This, however, could bring on the heating problems.

Visual Attack: one in every of the foremost direct attacks is ``spying" i.e., capturing the sunshine emissions from a show, led, or different device. Any sign or sensitive data ought to so be aloof from the visual illustration.

IV.CONCLUSION

The explosive growth of latest mobile-friendly applications and services is starting to create serious challenges to information security in mobile devices. Additionally, proliferation of such services among the mobile social networks will increase the probabilities for the user to be compromised and for a malicious attack to succeed. The aim of our analysis during this paper is to demonstrate that victimization cheap ready-to-wear instrumentality for side-channel attacks on the smart phones could be a serious threat, whereas such Associate in nursing intrusion remains arduous to observe. Specifically, our results reveal that even with low-end instrumentality the attackers already to observe signals of the crypto computations. In fact, as

shown within the latter a part of this paper, with solely a minor advancement within the attack tools its potential to amass even a lot of informative traces.

Therefore, sure-fire analysis of sensitive user knowledge represents a heavy threat for the non-public user data keep within a hand-held device that's connected through on-line services. For this reason, once illustrating a potential a lot of efficient attack that will be conducted to gather the information traces from alternative devices, we provide some tips that users could follow to decrease the amount of risk for his or her personal devices. As our future work, a potential extension here can be to extend the value of the attack instrumentality (while still residing among the common shopper segment), each on the hardware and software package sides, for sick the key keep within the mobile phones. Additionally, the used algorithms for parsing and classifying the traces can be improved more to leverage the extracted data even a lot of efficiently.

V. REFERENCES

[1]. L. Lin, L. Xu, S. Zhou, and Y. Xiang, "Trustworthiness-hypercube-based reliable communication in mobile social networks," Inf. Sci., vol. 369,34 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, architec-tures, 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 net-works: A hypergraph framework," IEEE Wireless Commun., vol. 23, no. 4,74 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 gami cation of advertising: Analysis and research directions of in-game advertising, advergames, and advertis-ing in social network games," J. Advertising, vol. 42, nos. 2 3, pp. 95 112, 2013