3-2012

HuMan: Creating Memorable Fingerprints of Mobile Users

Gupta PAYAS
Singapore Management University, payas.gupta.2008@smu.edu.sg

Kiat Wee TAN
Singapore Management University, kwtan.2010@smu.edu.sg

Narayanasamy RAMASUBBU
Singapore Management University, nramasub@smu.edu.sg

David LO
Singapore Management University, davidlo@smu.edu.sg

Debin GAO
Singapore Management University, dbgao@smu.edu.sg

See next page for additional authors

DOI: https://doi.org/10.1109/PerComW.2012.6197540

HuMan: Creating Memorable Fingerprints of Mobile Users

Payas Gupta*, Tan Kiat Wee*, Narayan Ramasubbu*, David Lo*, Debin Gao* and Rajesh Krishna Balan*
*School of Information Systems, Singapore Management University, 80 Stamford Road, Singapore 178902

***Abstract*—In this paper, we present a new way of generating behavioral (not biometric) fingerprints from the cellphone usage data. In particular, we explore if the generated behavioral fingerprints are *memorable* enough to be remembered by end users. We built a system, called HuMan, that generates fingerprints from cellphone data. To test HuMan, we conducted an extensive user study that involved collecting about one month of continuous usage data (including calls, SMSes, application usage patterns etc.) from 44 Symbian and Android smartphone users. We evaluated the memorable fingerprints generated from this rich multi-context data by asking each user to answer various authentication questions generated from the fingerprints. Results show that the fingerprints generated by HuMan are remembered by the user to some extent and were moderately secure against attacks even by family members and close friends.**

I. Introduction

Profiling or fingerprinting human behavior has been widely used as a technique in providing context awareness [1], intrusion detection [2], etc. However, there are many scenarios in which *memorable* fingerprints are desirable in profiling human behavior. One obvious application is in authenticating users who are not technically proficient. Memorable fingerprints are highly useful in these situations as they can be used to generate authentication questions that anyone can answer without memorizing or needing any physical device. Note that *memorable is usually more than memorizable*, i.e., a memorable fingerprint is one that can be recalled and recognized by human users, but is not necessarily one that needs to be memorized.

Memorable behavioral fingerprints are especially useful for context-aware applications as it is usually difficult to understand which aspect of a context a particular user deems most important, especially when the context is derived from multiple data sources or the various aspects are conflicting from one another. For example, a user might have two sets of nighttime behaviors. One is to call a friend at 10 pm while the other is to play a mobile game while calling. Which of these behavioral fingerprints is more important to the user? A memorable fingerprint would be more significant to the user and should be given higher weight. Users typically do not remember details of regular past events especially when they are not asked to memorize them. In this paper, we present HuMan: **H**istory-based **U**ser Centric **M**emorable **A**pplicatio**N** as an attempt for generating memorable fingerprints of cellphone users.

This research/project is partially supported by the Singapore National Research Foundation under its International Research Centre @ Singapore Funding Initiative and administered by the IDM Programme Office.

HuMan runs on the user's cellphone that monitors and records raw events, e.g., SMSes, calls, location, etc. Thereafter it processes the collected records and generates the memorable fingerprint e.g. "When a call is made, the callee is David". A good way to verify the memorability of these fingerprints with the user is through a question and answer format, e.g. "Whom do you usually call?". Thus, we developed a simple mobile authentication application to test the viability and usefulness of our fingerprints. The key features and contributions of the paper are:

- **Memorable fingerprints**: HuMan is the first attempt to generate memorable fingerprints from the users' cellphone usage behavior.
- **Multi-context data from cellphone usage**: HuMan generates fingerprints that are derived from data sources including call, SMS, email, calendar, application usage and browsing. We do this because fingerprints of different users are usually different.
- **Security protection**: We subject HuMan to a *difficult* security threat model where *intimates* (family members, close friends particularly those living with the participant) and *acquaintance* (casual friends, colleagues particularly those not spending a lot of time interacting with the participant) try to guess the fingerprints, and show that it provides *moderate* resistance to these threats. This is difficult as we expect family members and friends to be involved in a significant number of common activities such as calls and SMSes and are probably aware of a lot of user activities.

These features and contributions were validated via a user study involving 44 participants on two different phone operating systems (Symbian and Android). By analyzing results from the user studies, we shed light on the characteristics of memorable fingerprints and how they can be generated. To minimize the privacy risk as much as we can, HuMan masks out as much critical information as possible. For example, the content of SMS and email messages are *not logged*.

II. Related Work

There has been previous work that tries to understand the behavior of cellphone users [3], [4], [5]. Unlike those studies, HuMan is the first system which uses cellphone

usage data from multiple data sources to generate memorable profiles for the users. We now describe the differences from past studies in more detail.

Hong et al. studied the behavior of mobile data service users [4]. In our user study, we are also concerned with user behavior; however rather than investigating factors that affect their behavior, we would like to find memorable signatures that characterize their behavior. In another study, Hong et al. investigated models that determined mobile Internet usage [5]. Our fingerprints could also be viewed as a collective model of user behavior. In addition, we are concerned with the behavior of individual cellphone users and the construction of memorable fingerprints.

III. Architecture of HuMan

HuMan comprises of two modules; a data collection module and a fingerprint generation module (see Figure 1). The data collection module runs in the background on cellphones and unobtrusively logs all interesting user events. To produce fingerprints with rich entropy, HuMan collects a wide range of information on calls, applications, browsing, etc. This forms the base of HuMan with hundreds of thousands of data entries. The fingerprint generation module resides above the data collection module and consists of three sub-modules.

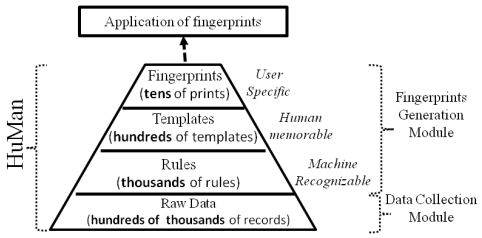

Figure 1. Architecture of HuMan

Data Collection

The data collection module (logger) runs unobtrusively in the background of the cellphone and captures a wide range of high level application events that result from user-phone interactions directly and indirectly. The events logged include Emails, Location, Calendar events, SMSes, calls etc. on Symbian (v3.0, 3.1 and 3.2) and Android (v2.1 and above) OSes. The development of the logger encountered some challenges. For example, we were limited by the available APIs on Symbian and the logger for Android makes use of the root access.

Fingerprint Generation

The data logged by our data collection module is in the form of raw events, e.g., call made to Bill at 8:12:32 pm and ended at 8:15:30 pm, which is harder to be remembered by human beings. Following are the steps to generate memorable fingerprints from raw events.

1) Machine-recognizable rules: We used standard association rule mining [6] and sequential rule mining [7] techniques to form machine-recognizable rules. For example the rules from association mining are of the form of "Whenever Raju calls Ankit, the duration is less than 1 minute". Similarly from sequential mining the rules are of like "Whenever Raju calls Ankit on Sunday, he calls David right after it".

2) Human-memorable rules: Not all rule components are easily memorable by human beings. Thus, to transform machine rules into a human memorable format, we first developed heuristics to rank the memorability of various types of information using a survey. We noticed that people could remember communication- (e.g., SMSes, calls) and application-based events (i.e. Apps) better. We also found that many people tend to remember *negative* rules (e.g. "you have *never* called X") and rules about *recent activities* ("application-X was the *last* one installed") well. We used these heuristics to create our base set of templates, which are in the form of rules with placeholders indicating information that can be easily memorable, e.g., "make a call to *X*". Fitting the machine-recognizable rules with the templates (an automatic process) is as easy as matching the placeholders in the templates with corresponding information in the rules.

3) User-specific fingerprints: The templates generated may not be user-specific (a template that says "You went to school at 9 a.m." could apply equally to multiple users). We thus manually filter the templates to pick the most user-specific templates (a fully automated version is future work). Finally, the small set of the most memorable template rules that do not overlap are combined to form the final fingerprint. We are still learning the best way to pick good template rules when forming the final fingerprint.

IV. Evaluation Methodology

We would like to evaluate the effectiveness of our fingerprinting approach to differentiate users from attackers. Also, we would like to find out what kind of fingerprints are memorable i.e. the one's related to a person/time/place etc. To evaluate HuMan, we installed our logger on the cellphones of participants for a period of 6 and 4 weeks for the Symbian and Android studies, respectively, to collect the raw data. Immediately after the data collection period, the participants were asked to bring along two persons, an *intimate* and an *acquaintance* for a lab study.

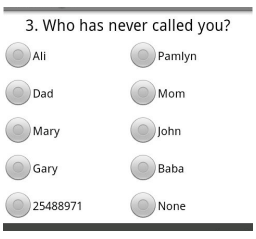

Figure 2. User Interface

To evaluate the memorability of fingerprints, we used the generated fingerprint as an authentication mechanism (see Figure 2). In particular, we translated the fingerprints into questions with reasonable candidate answers (e.g., a question involving names would pick the other name choices from the participant's cellphone's contact list). The ability of participants to answer these questions correctly gave us insights into the memorability of the fingerprints. Intimate's and acquaintance's answers gave us

insights whether fingerprints are actually resistant to attacks by people who know users the best. The intimate and the acquaintance separately and independently answered the same set of questions.

V. Symbian Study

We first discuss the study setup and results of this study, then present the lessons we learned as well as improvements made to HuMan as a result.

User Study Setup

As we decided to see if our scheme could replace standard authentication mechanisms, we decided to design the question-answering mechanism to have a similar guessing entropy of a standard 6-digit pin (a password space of 10^6). We designed three variants (6, 7, and 8 questions each with 10, 8, and 6 choices, respectively) of HuMan to test whether users preferred fewer questions with more choices versus more questions with fewer choices. The tradeoff is that with questions with fewer choices, answering each individual question might be easier, but the overall process takes longer. Conversely, having less questions with more choices might take less time overall, but answering each question is harder. We could not use less than 6 question with 10 choices as that would provide lower security guarantees than a 6-digit PIN. We cannot use free form question because it is harder for the machine to infer and verify (if the answer is correct or not).

In total we had 31 participants (10 male, 21 female) and their corresponding intimates and acquaintance from the undergraduate population at our university. 21 of the intimates spent between 4-8 hours per day with the participant while the remaining 10 intimates lived with the participant. Among the 31 acquaintances, 19 spent around 1-4 hours per day with the participant, while the rest saw the participant almost daily but did not really interact with him/her.

Results

We found no statistical difference (using t-test analysis for gender, technical qualification, etc.) in the accuracy of answers in all the 10-, 8-, and 6-choices variants. Therefore, we aggregated results from all three variants together in subsequent analysis.

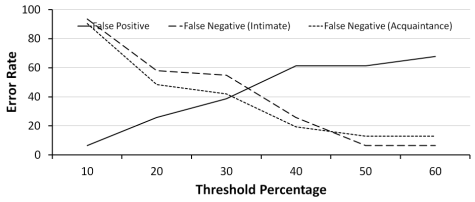

Figure 3. Symbian - false positive and false negative rates

We evaluated the accuracy in terms of false positive rate (when the participant was not able to login) and false negative rate (when intimates/acquaintances were able to login) for different threshold values (see Figure 3). The threshold is the percentage of questions a user/attacker needs to correctly answer to authenticate to the system. Unfortunately, we found that the threshold where false positive and negative rates meet (approx 40%) is quite low (approx 35%). To understand the reasons, we performed an in-depth analysis on the types of questions asked and brought them into 4 categories depending on the focus of the question (see Figure 4 for accuracy results).

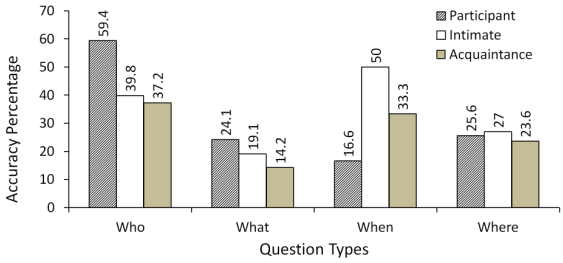

Figure 4. Effect of types of questions (Symbian)

Who: For example, "who do you call the most?" An accuracy advantage of the participant over potential attackers is because people tend to remember the interactions with other people.

What: For example, "what app do you usually use in morning?" By investigating deeper in the questions asked, we found that some of the choices were misleading. For example, our questions differentiated deleting "sent SMS" events from deleting "received SMS" events, whereas the participants could only remember that they deleted an SMS.

When: For example, "when do you usually call Bob?" This type of questions has a negative overall impact as intimates were able to answer them with even higher accuracy than the participant. Intuitively, this is possible when intimates spend a lot of time with the participant.

Where: For example, "Where do you usually charge your phone?" The where-type questions did not perform well and we discovered that the accuracy for this type of questions was high for the intimates.

VI. Android Study

We found that our participants' Symbian usage behavior was limited to calls and SMSes. Unlike Symbian, Android provides a richer set of multi-context data. In this study, we investigated if better fingerprints could be generated from the richer data-set.

User Study Setup

We asked participants to answer multiple-choice questions with the following characteristics:

1) We asked 6 questions with 10 choices each, to achieve the same security strength as a 6-digit pin. We did not consider other options as our Symbian study showed that there were no significant differences when 6, 8, or 10 choices were used.

2) We limited our generated questions to *Who* and *What*. In the Symbian study, participants performed better for these types of questions (see Figure 4).

In addition to undergraduates from our university, we also included working adults. In total, we had 13 participants (9 male and 4 female) out of which 9 were undergraduates (age between 19 and 25) and 4 (age between 24 and 33) were working professionals. 11 of the intimates spent between 4-8 hours per day with the participant while the remaining 2 intimates lived with the participant Among the 13 acquaintances, 4 spent around 1-4 hours per day with the participant, while the rest saw the participant almost daily but did not really interact with him/her.

Results

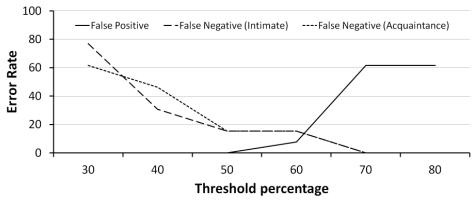

Figure 5. Android - false positive and false negative rates

Figure 5 shows the false positive and false negative rates of the test. This is a big improvement over the Symbian results. We were able to increase the threshold to 61.8% while decreasing both the false-positive and false-negative rates to approximately 15.3%. The improved accuracy was due to the changes in the user study design as well as the richness of the android multi-context data-set. One possible reason why intimates and acquaintances are still able to answer many questions correctly could be because they can observe a person and thus know a lot of details about the person peculiar habits and characteristics.

VII. Discussion

Characteristics of Memorable Fingerprints

Our user studies were a great learning process to allow us to understand the characteristics of memorable fingerprint.

Broad Range of Events Necessary: Symbian users hardly used their phones for anything but SMSes and calls, from which very few memorable signatures could be constructed. On the other hand, Android provided more event types including applications, emails, which allowed us to recover more memorable fingerprints.

Use the Most Memorable Templates: We quickly realized that certain events are more memorable than others. We categorized our templates based on the type of information they contained, i.e., "who", "what", "when", etc. In our experiments, we consistently found that the templates containing "what" and "who" types were more memorable. We also found that certain special types of fingerprints performed well, e.g., those representing negative rules.

Limitations

Through our exploration with the fingerprints, we believe that our user study provides a good test on the memorability of fingerprints generated by HuMan and we also note some of the limitations discovered through this exploration.

1) *Trade-off between Power/Performance.* There was an inevitable minor issue on Android with regards to the tradeoff between the slight lag in performance and power drain due to the increase logging of more data.
2) *Authentication.* In authentication scenarios where a system requires frequent authentication, the current version of HuMan may not be the best fit because of moderate accuracy and the time to answer one question (9 seconds on average) as compared to 8.46 seconds on average to enter a 6 digit PIN (based on our tests). However, some authentication scenarios where HuMan is suitable might be 1) when the phone is lost and needs to be locked remotely. 2) to unlock or change the SIM card.

VIII. Conclusion and Future Work

In this paper, we looked at the usefulness of memorable cellphone fingerprints. We designed HuMan, that uses cellphone usage patterns to generate memorable fingerprints. We described the components of HuMan and presented detailed user-based. This evaluation used Symbian and Android OSes to understand the design criteria needed for generating memorable fingerprints along with the effectiveness of these fingerprints in an authentication scenario.

The current state of HuMan could achieve false positive and negative rates of approximately 15.3%, and might not be able to replace existing authentication systems in places which require frequent authentication. However, what we found was encouraging and opens numerous avenues for further exploration and research. Moving forward, we plan to continue our research into human-centric approaches in generating quality fingerprints in a number of ways: 1) testing HuMan with a broader and more diverse set of users; and 2) deploying it to other areas, beyond authentication, such as context-aware profile systems. 3) analyze the scenario when the attacker has a complete log of the data communication from and to the cellphone.

References

[1] M. Baldauf, S. Dustdar, and F. Rosenberg, "A survey on context aware systems," *IJAHUC*, vol. 2, June 2007.
[2] R. V. Yampolskiy, "Human computer interaction based intrusion detection," *ITNG*, vol. 0, 2007.
[3] B. Kim, M. Choi, and I. Han, "User behaviors toward mobile data services: The role of perceived fee and prior experience," *ESWA*, vol. 36, May 2009.
[4] S.-J. Hong, J. Y. L. Thong, J.-Y. Moon, and K.-Y. Tam, "Understanding the behavior of mobile data services consumers," *Information Systems Frontiers*, vol. 10, Sep 2008.
[5] S.-J. Hong, J. Y. L. Thong, and K. Y. Tam, "Understanding continued information technology usage behavior: a comparison of three models in the context of mobile internet," *Decis. Support Syst.*, vol. 42, Dec 2006.
[6] R. Agrawal and R. Srikant, "Fast algorithms for mining association rules." in *Proceedings of the International Conference on Very Large Data Bases (VLDB)*, 1994.
[7] D. Lo, S.-C. Khoo, and L. Wong, "Non-redundant sequential rules – theory and algorithm," *Information Systems*, vol. 34, pp. 438–453, 2009.