User Profiling through NFC interactions: Mining NFC-based User Information from Mobile Devices and Back-end Systems

Anders Andersen, Randi Karlsen
Department of Computer Science
Faculty of Science and Technology
UiT The Arctic University of Norway
9037 Tromsø, Norway
{Anders.Andersen,Randi.Karlsen}@uit.no

ABSTRACT

With the myriad of information resources available on the Web, personalization has become important to facilitate information retrieval and recommender systems that provide information and services adapted to the user's needs. A crucial component in any personalization approach is the availability of a user profile that reflects the user's interests, behaviour and intention. In this paper we exploit the fact that for many people the mobile phone is a close companion that follows the person everywhere and is used for many different tasks in the person's daily life. In particular, we focus on mining user activities on NFC-based services to collect information that can be included in a user profile. The paper describes the process of mining usage information from multiple NFC-based applications, both on a smart phone and on back-end systems. We also describe our experiments that lead to and support mining of NFC-based user information.

1. INTRODUCTION

With the huge amount of information and services available on the Internet, personalization has become an important tool for assisting users in searching, filtering and selecting items of interest. Personalization is described as the ability to provide tailored content and services to individuals based on knowledge about their preferences and behavior [1].

User profiling is necessary to identify user interests, behavior and other characteristics that can later be used for personalization. To construct a user profile, information can be collected *explicitly*, through direct user participation, or *implicitly*, through automatic monitoring of user activities [2]. Implicit gathering of user information, which is the focus in this paper, traditionally includes systems that automatically infer user interests or behavior by keeping track of the user's search history in terms of submitted queries and clicked results, processing of stored documents, and harvesting of information from the user's interaction with social applications [2]. In this paper we expand the sources for implicit user information to include *NFC-based user activity information*.

Near Field Communication (NFC) is used in mobile applications to provide easy and convenient access to information and services. This short range communication can facilitate exchange of information and/or trigger execution of services. NFC interaction has been described as "the deliberate bringing together of two devices, for the purpose of obtaining services" [3]. NFC is used in a wide range of applications that cover many aspects of a user's daily life activities [4]. This includes payment and loyalty card applications, access keys (e.g. for offices and hotel rooms), ticketing, and various forms of information services (such as smart posters, location-based wikis and applications of NFC in tourism [4, 5, 6]).

We believe that the variety of NFC applications, accessed through a single personal device (such as a smart phone), collectively may provide very useful information concerning user activity and interests. We also believe that NFC-based services are particularly well suited for user profiling as information can be implicitly gathered, while they also inhibit some of the preciseness of explicitly provided information. The touch of an NFC tag represents an explicit action including an implicit statement of interest.

In the following, we focus on how NFC interactions can be intercepted in order to mine user activity information. We describe the process of mining usage information both on a smart phone and on back-end systems, and describe some of our experiments that lead to and support mining of NFC-based user information.

2. NFC-BASED USAGE MINING

Near field communication (NFC) is a set of short range wireless technologies that limits communication to distances below 10 cm (typically 4 cm) and is established by devices (almost) touching [7]. There are in general three types of NFC devices; NFC mobile phones, NFC tags and NFC readers [7], and the communication involves an initiator and a target.

In the simplest NFC use-cases, the smart phone acts as the initiator, and by touching an NFC tag it can read or modify information on the tag. By mining this information on the smart phone, user interests can be inferred.

MobiWac'16, November 13-17 2016, Malta, Malta

ISBN 978-1-4503-4503-3/16/11...$15.00

DOI: http://dx.doi.org/10.1145/2989250.2989274

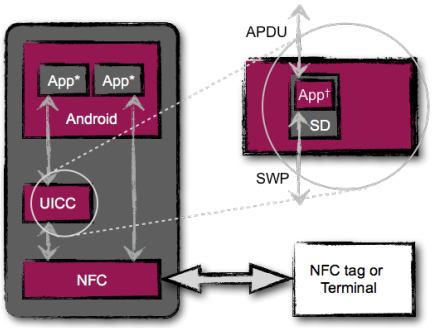

Figure 1: NFC-enabled Android smart phone.

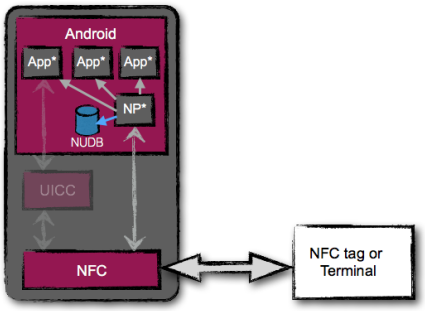

Figure 2: The NFC proxy NFC usage collection.

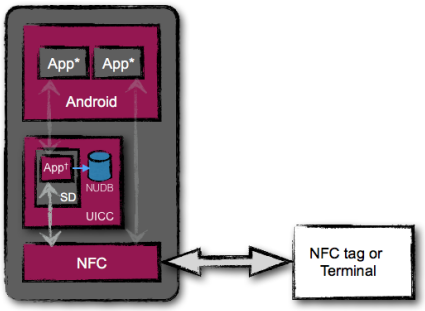

Figure 3: The card emulation NFC usage collection.

In a different use-case, a user enters a bus and uses a smart phone to touch an NFC-enabled ticket machine to validate the ticket stored on the smart phone. The ticket machine is in this case the *initiator* and the smart phone is the *target* responding to the ticket machine with a ticket that can be validated.

Information about this interaction can be collected in the ticket machine (the initiator) and in the smart phone (the target). However, such an interaction might involve a back-end system, where information about the interaction can be collected and stored.

In the following, the details on how to mine NFC usage information at mobile devices and back-end systems are described.

2.1 NFC usage mining at mobile devices

How to collect information about NFC usage depends a lot on the type of device in use. We focus here on smart phones, and in particular on Android smart phones. Similar approaches are in principle possible on other devices and on non-Android based smart phones.

Figure 1 illustrates the components of a smart phone that can be involved in the NFC interaction. Android apps (App* in the figure) are executed in the Android subsystem. They can communicate with NFC tags or other NFC devices using the NFC subsystem on the smart phone. Universal Integrated Circuit Card (UICC) is an embedded smart card on the phone. It contains apps (App† in the figure) executed in secure domains (SD). The Subscriber Identity Module (SIM) is an example of such an app[1]. UICC apps can be used to implement secure elements (SE), and can communicate directly with NFC tags and other NFC devices using the Single Wire Protocol (SWP) to the NFC subsystem. Android apps can communicate with the UICC and UICC apps using Application Protocol Data Unit (APDU) commands.

On the Android subsystem different applications can use NFC to interact with an NFC tag or other NFC devices. Such an app can register to be activated when an NFC tag of a given type [8] is detected by the NFC subsystem on the phone. In practice, this means that when the user touches a tag of a given type with the smart phone, the registered app will be activated and provided the data from the NFC tag. The smart phone is in this case the initiator initiating the communication with the NFC tag. Based on the type of the tag, the Android tag dispatch system[2] delivers the intent to the correct registered app.

To mine the NFC usage on the device, we have developed a helper app, called NFC Proxy (NP), that is registered to handle all NFC tag types that is relevant for mining usage information. NP collects the usage data in an NFC-usage Database (NUDB), and then activates and provides the data to the actual app that is handling this type of NFC tag. Figure 2 illustrates this approach.

The information stored can include a time stamp, the intent (e.g. a URL or an ID), location (from GPS or other location services), the Android app that will receive the intent, and more details related to the current context (e.g. phone in do-not-disturb mode, specific Android apps, like music player and training diary, active, and so on).

In a typical configuration, the Android dispatch system is active when the device is on and the screen is unlocked. This means that the NFC enabled smart phone is a potential NFC initiator when the phone is on and the screen is unlocked. However, the phone can be an NFC target when the screen is locked (back-light is off), or even when the phone is turned off. In such cases only the UICC and the NFC subsystem are involved in the NFC interaction. The typical usage for such NFC interactions are ticketing, payment and door unlocking. In these cases the external terminal (e.g. ticketing machine) is the initiator and the smart phone is the target. The NFC subsystem on the phone forwards the NFC request to a card emulator app on the UICC. This app behaves like a payment card, an electronic ticket, or a key card. Figure 3 illustrates this use-case. In such NFC interactions, the Android subsystem is not involved at all.

[1]The UICC on a mobile phone is often referred to as the SIM card since the SIM app represents the original purpose of the UICC.

[2]`http://developer.android.com/guide/topics/connectivity/nfc/`

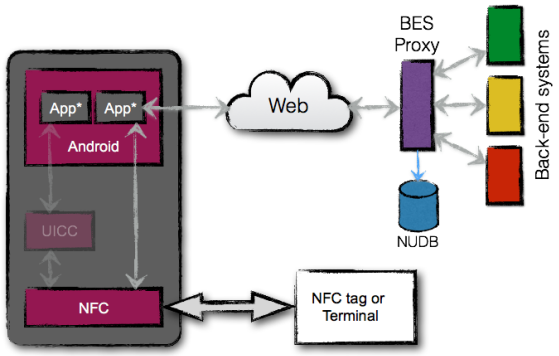

Figure 4: The Back-End System (BES) proxy collecting NFC usage in a NUDB.

ID	URL
1000	`https://back-end-a.net/`
1001	`https://back-end-b.net/one`
1002	`https://back-end-b.net/two`
1003	`https://back-end-c.net/?sys=pay`
1004	`https://back-end-c.net/?sys=track`

Table 1: A BES proxy forwarding table.

This NFC usage can be directly collected if the app on the UICC stores this information in its local NUDB. The usage can also be collected in the external NFC device or at an end-system.

UICC apps are considered more protected from intrusion than Android apps [9]. The main reasons is that they are executed on secure domains inside tamper resistant UICC smart cards. The interaction with UICC apps also follows a tight authorization scheme. This is one motivation for using UICC for payment, ticketing, and electronic door keys. Details on this is out of the scope of this paper.

The user profiling process needs access to usage data collected at each UICC app. One way of achieving this is to make the NFC Proxy (NP) or another Android App periodically collect this data from all registered UICC apps. This can only be achieved if such an Android App is authorized access to the secure domain (SD) of the UICC apps of interests.

2.2 NFC usage mining at back-end systems

NFC tags or applications accessing a back-end system as a result of an NFC interaction are identifying the back-end system using an URL scheme. For a given user this might involve a large number of back-end systems running on a large number of different servers with different locations. To be able to collect this data at a single NUDB, a Back-End System (BES) proxy is introduced. All tags and applications are accessing their back-end systems through this BES proxy. Figure 4 illustrates the BES proxy setup. The BES proxy includes a forwarding table for each type of back-end system that includes the actual URL for the back-end system. Table 1 is an example of such a forwarding table. Assuming the BES proxy has the URL `https://www.besproxy.net/`, Table 2 shows the request sent to the BES proxy from the NFC device and the resulting address the request is forwarded to after the NFC usage data are collected in a NUDB.

The BES proxy approach makes it possible to collect all back-end system interaction in a single NUDB, and it provides the flexibility of adding or modifying involved back-end systems. For example, if a user with the smart phone touches an NFC tag containing a web-address, the browser on the phone could open a web page that contains information about the object with the attached NFC tag. With the BES proxy in use, the host name of the URL on this tag is the host name of the BES proxy. The web-browser on the phone opens this URL, the BES proxy collects the NFC usage data in the NUDB, and finally the BES proxy forwards the web-browser to the actual web page with the information. Nothing on the smart phone is in this case involved in mining the NFC usage data.

```
https://www.besproxy.net/1002
→ https://back-end-b.net/two
https://www.besproxy.net/1000?op=get&art=129
→ https://back-end-a.net/?op=get&art=129
https://www.besproxy.net/1004?reqid=14&par=12
→ https://back-end-c.net/?sys=track&reqid=14&par=12
```

Table 2: Examples of URL mapping in BES proxy.

3. EXPERIMENTS

The insight and examples presented above is the result of a series of experiments and projects regarding NFC, context awareness, and user profiling. In the NFC City project[3] and the CAIM project[4] we have performed several experiments mining user activities. In [10, 11, 12] different types of NFC applications and experiments in the context of the NFC city project are discussed, while in [13] image annotation using NFC in the context of the CAIM project is discussed. An example of how to store activity and interest information on an NFC tag is also found in [13]. In [14, 15, 16] topics concerning NFC, mobility and security are discussed.

In the NFC City project analyses of NFC usage and the user experience with NFC usage was important [12]. This led to the development of a web-proxy similar to the BES proxy discussed above. Initially, this was only used to mine anonymized usage data for NFC usage research. Later, it was extended so support the mining of user activities at back-end systems for better user profiling.

However, one problem with the BES proxy approach is to identify the user. The HTTP request will include an IP-address of the smart phone that is obtained from a pool of addresses (managed by a DHCP server) and therefore cannot be used to uniquely identify the device/user. In the NFC city project experiements [10, 11] it was ensured that each participating NFC enabled smart phone got a unique IP address both on the local network and on the telecom operator's LTE/3G network. To assign unique IP-address to devices might not be feasible in the general case, and other approaches were considered in the NFC city project. This included usage of web cookies and inserting identifying information in HTTP request headers. However none of this approaches were possible in the general case without doing special preparation of the devices and/or introducing user ID and log in at the services.

In the NFC City project, the usage of the UICC for a set of security critical NFC applications [14, 15, 16] introduced new challenges to user activity mining. As discussed

[3]http://www.telenor.com/t/nfc-city/
[4]http://caim.cs.uit.no

above, it is possible to collect the usage data by introducing a NFC-usage Database (NUDB) at the UICC. Since the UICC apps are running secure domains (SD), one possible implementation is to have a separate NUDB per app, and synchronize this data with an Android app running in the Android subsystem. This could either be with an Android app for that specific services, or with the NFC proxy (NP).

In our experiments one concern was privacy. To support this we tried to limit the amount of data stored on the BES proxy NUDB, and all data for a given user in the NUDB is stored encrypted with a public key. The matching private key is only available on the user's mobile phone. The consequence is that these data can only be decrypted and accessed on this mobile phone. This implies that the processing of NFC usage data to generate and update a user profile is done at the user's mobile phone. When this processing occurs, data from the NUDBs in the Android subsystem and from the NUDB on the BES proxy relevant for this user are made available to the process. The relevant data from the BES proxy has to be transferred to the mobile phone of the user.

4. CONCLUSION

Up to date user profiles are a crucial component for personalization of services and applications. In this paper we have identifies NFC usage as a contributer to the creation and updates of user profiles. We have described how NFC usage mining can be performed on the mobile device and on the back-end system. We have also discussed NFC usage mining in practice, where we combine usage mining at mobile devices and back-end systems, and how the NFC experiments in the NFC City and CAIM project contributed to this.

5. ACKNOWLEDGMENTS

The authors appreciate the support from the Norwegian Research Council (NFR) through the *Context-Aware Image Management* project (CAIM, NFR project number 176858) and the *NFC City* project (NFR project number 201377). We would like to thank partners, project members and students of the NFC City and CAIM project who created a perfect environment for our research.

6. REFERENCES

[1] M. Gao, K. Liu, and Z. Wu, "Personalisation in web computing and informatics: Theories, techniques, applications, and future research," *Information Systems Frontiers*, vol. 12, pp. 607–629, Nov. 2010.

[2] M. Ghorab, D. Zhou, A. O'Connor, and V. Wade, "Personalised information retrieval: survey and classification," *User Modeling and User-Adapted Interaction*, vol. 23, no. 4, pp. 381–443, 2013.

[3] J. Bravo, R. Hervas, G. Chavira, S. Nava, and V. Villarreal, "From implicit to touching interaction: RFID and NFC approaches," in *2008 Conference on Human System Interactions*, pp. 743–748, May 2008.

[4] K. Ok, V. Coskun, M. Aydin, and B. Ozdenizci, "Current benefits and future directions of NFC services," in *Education and Management Technology (ICEMT), 2010 International Conference on*, pp. 334–338, Nov. 2010.

[5] E. Siira, T. Tuikka, and V. Törmänen, "Location-based mobile wiki using NFC tag infrastructure," in *First International Workshop on Near Field Communication (NFC'09)*, pp. 56–60, IEEE, Feb. 2009.

[6] J. Pesonen and E. Horster, "Near field communication technology in tourism," *Tourism Management Perspectives*, vol. 4, pp. 11–18, 2012.

[7] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (NFC) technology," *Wireless Personal Communications*, vol. 71, no. 3, pp. 2259–2294, 2013.

[8] NFC Forum, "NFC data exchange format (NDEF)," Technical Specification NDEF 1.0, NFC Forum, July 2006.

[9] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC devices: Security and privacy," in *Third International Conference on Availability, Reliability and Security, ARES 08*, pp. 642–647, Mar. 2008.

[10] A. Andersen and R. Karlsen, "Experimenting with instant services using NFC technology," in *The First International Conference on Smart Systems, Devices and Technologies (SMART 2012)*, (Stuttgart, Germany), IARIA, May 2012.

[11] A. Andersen, R. Karlsen, and A. Munch-Ellingsen, "NFC provided user friendliness for technologically advanced services," in *15th International Conference on Human-Computer Interaction (HCI International 2013)* (S. Yamamoto, ed.), vol. 8017 of *Lecture Notes in Computer Science*, (Las Vegas, USA), pp. 337–346, Springer-Verlag, July 2013.

[12] B. Evjemo, S. Akselsen, D. Slettemeås, A. Munch-Ellingsen, A. Andersen, and R. Karlsen, "I expect smart services! – user feedback on NFC based services addressing everyday routines," IFIP Transactions, (Rome, Italy), Oct. 2014.

[13] R. Karlsen and A. Andersen, "NFC-based image annotation," in *The International Workshop on the Future Internet of Things and Cloud (FiCloud 2013), in conjunction with The 10th International Conference on Mobile Web Information Systems (MobiWIS 2013)* (M. Matera and G. Rossi, eds.), vol. 183 of *Communications in Computer and Information Science*, (Cyprus), pp. 72–85, Springer-Verlag, Aug. 2013.

[14] A. Andersen and A. Munch-Ellingsen, "Mobile device security: The role of NFC, UICC and secure elements," in *Norsk Informasjonssikkerhetskonferanse (NISK 2014)*, (Fredrikstad), Nov. 2014.

[15] A. Munch-Ellingsen, A. Andersen, S. Akselsen, and R. Karlsen, "Customer managed security domain on mobile network operators' SIM cards: Opportunities to enable new business models," in *Marktplätze im Umbruch: Digitale Strategien und das Zusammenwachsen von Shop, Online-Business sowie Services im Mobilen Internet*, Springer-Verlag, 2015.

[16] A. Munch-Ellingsen, R. Karlsen, A. Andersen, and S. Akselsen, "Two-factor authentication for android host card emulated contactless cards," in *Proceedings of the 2015 First Conference on Mobile and Secure Services (MOBISECSERV)*, 2015.