YOUR MOBILE PHONE IS A TRAITOR! – RAISING AWARENESS ON UBIQUITOUS PRIVACY ISSUES WITH SASQUATCH

Bram Bonné, Peter Quax and Wim Lamotte

Hasselt University – tUL – iMinds, Expertise Centre for Digital Media
Wetenschapspark 2, 3590 Diepenbeek
{bram.bonne, peter.quax, wim.lamotte}@uhasselt.be
Belgium

Abstract: Smartphones may leak personal information about their owner through the built-in Wi-Fi hardware. Most importantly, the list of networks the device has previously been connected to is exposed. Based on this seemingly harmless information, one can not only infer a person's whereabouts but also create a clone of a network the smartphone is trying to connect to. Previous studies have shown that users are often not aware that this information is being leaked. In order to raise awareness about this problem, we have designed a setup consisting of a network scanner and a public display, which alerts users about this problem by displaying private but anonymized information. The setup contains an interactive component which allows people to view the information their own smartphone is leaking, and presents them with a short guide on how to configure their device for increased privacy and security. When asked about their privacy concerns and about their willingness to secure against privacy leaks, we found out that 90% of the participants were worried about information as displayed leaking to third parties, with 81% indicating that they were willing to put an extra effort into securing their smartphones.

Key words: privacy; security; mobile; wireless

1. INTRODUCTION

The revelations of whistleblower Edward Snowden about the large scale collection of private data by the US National Security Agency have shown that our mobile phones can be used as devices that gather personal information about their users. Despite the predominant public opinion that this type of data collection is

only possible for large organizations with world-wide networks, illicit data gathering can be done with a fairly simple setup using off-the-shelf wireless hardware. The strategies currently used by mobile operating systems to search for and connect to available wireless networks involve openly sharing a list of previous accessed networks. While this might seem harmless, these strategies may reveal the smartphone user's name, workplace, standard network provider, previous visited locations and even social relationships [1]. Worse, an attacker can use the name of a network the victim's smartphone connected to in the past, impersonate it and retrieve login information for private websites [2]

In recent work, Könings et al. propose a model to enhance user-centric privacy awareness [3]. Three core questions are put forward in this work that contribute to the understanding of privacy: who is affecting my private data, what is the purpose (why) and how is it being accomplished. Most mobile phones, however, openly share their list of previously accessed networks to increase the comfort and ease of use for the end-users but fail to inform the users about the consequences. A study performed in 2009 by Klasnja et al. shows that users are unaware of important privacy risks when using Wi-Fi networks [4]. An interesting result in this study is that many of the participants thought about a hacker as a highly skilled attacker who breaks into their computer, and not as someone who can passively collect their data when it is sent over the network. The fact that people are in general very susceptible to Wi-Fi attacks is confirmed by Kindberg et al., who were able to mount a phishing attack on the login page of a public hotspot, tricking 32% of users connecting to their own fake hotspots into entering their mobile phone number [5].

Other work shows that, when confronted with possible privacy concerns, people are willing to act in the interest of preventing further privacy leaks. A survey of 2254 participants by Boyles et al. [6] demonstrated that 57% of all smartphone app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons. An empirical study by Günther et al. [7] assessing the privacy fears related to using Radio Frequency Identification (RFID) showed a similar trend: 73% of 129 retail consumers preferred RFID to be disabled on checkout. Moreover, results presented by Consolvo et al. [8] show that a user's privacy awareness can be increased by showing the user personal information that is unwittingly shared.

In this work, we describe a system called SASQUATCH that collects privacy-sensitive information that is sent out inadvertently by people's smartphones. The main contributions are as follows:

1. We explore whether people can identify themselves when we show them information that is contained in a list of previously accessed networks.
2. We create user awareness about potential privacy and security issues when a smartphone connects to Wi-Fi networks.

3. We assess the effort the average smartphone user is willing to invest in securing against privacy leaks.
4. We explain to smartphone users (and to the readers) what can be done to secure against privacy and security issues.

For this purpose, we combined SASQUATCH, our system that gathers data from mobile phones and impersonates networks, with a public display that pictures the data that is captured. The visualizations used are, of course, anonymized and carefully abstracted.

2. MOBILE PHONES THAT "NEVER FORGET"

For long, mobile phones have been thought of as "trusted devices": they are used for private communication, coupled to a single user. However, in a time where smartphones dominate the mobile landscape, this trust is often unfounded. In reality, smartphones are known to collect all kinds of data – ranging from a user's contacts to precise location data – via many different channels. For example, leaked documents by Edward Snowden show that popular smartphone apps were targeted by the NSA and GCHQ because of the vast amounts of user data they collect (as published in *The Guardian* on January 27 2014). In another example, marketing agency "Renew" used trash cans in London to track people via their smartphones' Wi-Fi signals. This data leakage is in part due to functionality that provides convenience for the smartphone user, such as the mechanism that relieves users of the task of manually searching for known Wi-Fi networks, or services automatically logging in and looking for new data (e.g. mail clients or social network applications). This trade-off between usability and security is a long known problem in the security community [9].

In our first study, which was performed at an international music festival in 2013, we collected information from smartphones of over 40000 festival visitors (about 47% of the amount of tickets sold). The system we used to collect this amount of information is WiFiPi [10], which is also the foundation of SASQUATCH. WiFiPi collects Wi-Fi signals sent out by smartphones at multiple strategic locations on the festival terrain. By using the unique smartphone identifier (*MAC address*) contained in each of these Wi-Fi packets, and correlating captured signals at different locations, we were able to track visitors over the entire festival area. Based on anonymized data we could infer which music stages a person visited at what time. We were able to cluster visitors based on their musical preferences, and we generated association rules that could be used to infer which artists a visitor was most likely to visit based on other attended performances.

We also used our WiFiPi system to collect lists of the networks that users had connected to in the past (how this can be done will be explained in section 3). This led to some interesting results: of the 40815 devices that we detected during this event, 23103 devices (50.60%) sent out at least one network identifier (SSID).

Moreover, 6609 of these devices (28.61%) broadcasted at least one network that was not broadcasted by any of the other devices, and more than 50% of the devices contained an SSID that was shared among at most 50 other devices. This means that nearly a quarter of the people carrying a smartphone could be uniquely identified only by the list of networks in their phone, and that clustering people by workplace or home based on the gathered data is possible. We were able to achieve these results with a simple and low cost setup, which underscores the fact that anyone with limited resources could collect similar data at any particular location.

Similar to results by Klasnja et al. [4], we noticed that most people are not aware of this information leakage. In a short pre-study in our lab environment we were able to identify a significant number of our own colleagues (researchers with a background in computer science) solely based on the network SSIDs sent out, the manufacturer of the smartphone or the time at which they entered or left our lab building. We confronted 10 colleagues with this information. All but one of them indicated that they were not aware that this information was so easily obtainable. This is not surprising, as many smartphones do not display the list of known networks. Devices running iOS in particular only show a stored network name when it is in range, leaving users in the dark about which information is leaking from their phones.

3. THE SASQUATCH SYSTEM

The method that is used by modern smartphones when scanning for known (or 'remembered') networks is known as 'active scanning'. It works as follows:

1. Send out a probe request for the first 'remembered' network in the smartphone's preferred network list (PNL).
2. Keep the Wi-Fi radio powered on for a short amount of time, listening for access points sending probe responses.
    a. If a probe response is received, initiate a connection with the network.
    b. If no probe response is received within the chosen time window, go back to step 1 while choosing the next network in the PNL.
3. When arrived at the last network in the PNL, put the Wi-Fi radio to sleep for *n* seconds (the *probe request interval*).

SASQUATCH consists of a single machine capturing all probe requests that are sent out by smartphones in range. The information obtained through this mechanism is used in three ways:

- The SSIDs of the networks broadcasted by a user's smartphone are used to create a profile of the user. This is done not only by gathering the network names, but also by looking up the SSIDs of these networks in the `WiGLE.net` wardriving database (available at http://wigle.net), which

allows to find the specific locations of access points. These locations are used to make an educated guess (calculated via the method outlined in section 3.1) about the user's whereabouts.

- The system executes an Evil Twin attack [2], impersonating networks in the smartphone's PNL, in order to identify which networks correspond to open access points. How this method works, and how it can be used to identify open networks is discussed in section 3.2.
- The manufacturer of the smartphone is derived from the Wi-Fi packets by deriving the Organizationally Unique Identifier (OUI) from the MAC address in each packet. The system performs a lookup for this identifier in the OUI list, kept up to date by IEEE (and available at http://standards.ieee.org/develop/regauth/oui/oui.txt).

3.1. Inferring a smartphone's whereabouts

Since the SSIDs of wireless networks may be used by multiple access points (often located at different locations), there is no one-to-one mapping of networks and locations. To make an educated guess about a subject's visited locations, we combine both types of networks (open as well as secured) as follows:

1. For every network in the smartphone's PNL, query `WiGLE.net` for a possible list of locations, returned as *(latitude, longitude)* tuples. Assign to every one of these locations a chance of *1/n*. For instance, because the SSID `UHasselt-Guest` returns 19 possible access points at different locations, we assign to each of these locations a chance of *1/19*. This chance only depends on the number of results for the *current network*, and is in no way related to the number of locations returned for other SSIDs in the subject's PNL.
2. At this moment, we have no way of telling whether any or all of these locations are results for access points at the same location. This will be accounted for in the next steps.
3. Use Google's *reverse geocoding* API to infer the city corresponding to the *(latitude, longitude)* tuple returned by `WiGLE.net`. For instance, given that the first result returned for SSID `UHasselt-Guest` is the tuple *(50.93173981, 5.39291286)*, we infer that this network has a *1/19* chance of being located in Diepenbeek.
4. Combine the locations of all of the smartphone's networks to deduce the chances that the user visited a certain location, by assigning every location a value that is the sum of the chances that any of the networks is situated at this location, as follows:

$$p_{city} = \sum_{networks} p_{(city,network)}$$

The resulting value should not be thought of as a mathematical probability, since it is possible that it is larger than 1. Rather, the value gives an indication on the probability that the device effectively visited a specific city. We discuss how this value is used to assess whether a device visited a certain location below.

Even if multiple networks have only a small chance of individually being associated with a certain city, together they can be used to infer that a person went to that city with high probability. For example, assume that network has a chance of only 0.5 at being located either city or city, and network has a chance of 0.3 at being located in either one of cities. It can then be inferred that the user has a high probability of having visited city. Moreover, networks that return different possible locations may have a majority (or all) of them located at the same approximate location (e.g., because there were multiple hotspots with the same SSID in the same building). This is also accounted for by recombining the location chances in the last step.

SASQUATCH determines a device to have been at a location if the resulting value for that location is strictly greater than 0.5. The reasoning behind this is as follows: if a network is available at two or more locations, the maximum possible chance assigned to a specific location is 0.5. Therefore, at least two networks are needed to obtain a chance > 0.5. A similar case can be made for networks that exist at four locations (at least four are needed), and so on.

3.2. Determining a network's authentication type

Probe requests only contain the SSID of the network they want to connect to, omitting the type of authentication that will be used for this connection. This authentication information is only available as part of the probe response, sent out by the access point.

Because probe requests do not contain an authentication type, SASQUATCH sends out a probe response as if it is an open network for every probe request it received, effectively pretending to be an open network in the smartphone's network list. Then, when a smartphone tries to connect to SASQUATCH (by sending out an *association request*), our system can infer that the network with the SSID contained in the probe request is indeed an open network. This method of tricking devices into connecting to an access point by pretending to be a known network is known as the Evil Twin attack [2].

Our system stops here: smartphones that try to connect to SASQUATCH are prevented from connecting by not acknowledging their association request. A person with malicious intent, however, can continue from here and set up a successful attack: as soon as a smartphone connects to one of the spoofed networks, this attacker is an *active man in the middle*. This allows the attacker to capture the smartphone user's data, even when it is sent over encrypted (SSL) connections [11]. This is especially worrying with smartphones, where many applications continuously check for new information in the background.

4. STUDY

We have performed a field study in which we explored whether people can recognize themselves if bits of information retrieved from their smartphone are displayed, assessed the level of awareness people have about the "open nature" of their smartphones, and evaluated the people's willingness to secure their smartphones against information leakage. Based on this, our hypotheses are that (1) people will be able to recognize themselves when their data is shown, (2) people are unaware about the amount of information being shared by their smartphones, and (3) people are willing to put a minimal effort (e.g. installing an app) in securing their smartphones. The apparatus we deployed for our study is a public display that shows the data gathered by SASQUATCH. The public display setup consists of two parts: a large display for public usage and a smaller one that can be used individually (see Figure 1):

- The large public display shows both the aggregated locations and the insecure (open) networks of all smartphones that were in range in the past 5 minutes.
- The smaller display shows the information that was inferred from a single smartphone. Viewers are invited to give consent for displaying their information by performing an action.

Fig. 1. The setup, as it was deployed at our research institute. The main screen, displaying aggregate information about all smartphones in a range of 50 meters is shown on the left. To the right of this screen is another (smaller) screen, on which a smartphone user can choose to display the information our system gathered form his/her smartphone.

The public display visualization was designed to trigger a "honeypot" effect [12], i.e. to entice people to start interacting with the screen. The map-based

visualization in combination with a list of names of networks (see Figure 2) made it easy for people to recognize (part of) themselves on the display while remaining anonymous.

Fig. 2. A screenshot of the information available on the public display. The top of the page shows the aggregate locations for all devices, together with a heat map of these locations. The bottom of the page shows a list of open networks devices wanted to connect to, and an invitation to partake in the study.

Participants in our field study were passers-by that were drawn to the screen out of curiosity because of what they noticed on the screen. We also had an assistant that stimulated people to look at the display. We distinguish between *passive participants*, participants that inspected the public display but did not interact, and *active participants* who actively engaged with the setup to view the information that was shared by their smartphones.

We deployed our apparatus at two different locations: our research institute entrance hall and the university's main hall. The setup was active for several days at the research institute and attracted 51 active participants over the course of a week. At the university's main hall we deployed the system for one day and we attracted 31 active participants. We estimate the number of passive participants is three to five times the number of active participants (no counts were done of passive participants).

The public display (see Figure 2) is designed in a manner similar to work by Kowitz et al. [13], in that it aims to strike a balance between notification and privacy. We achieve this by having the display show a list of locations that any of

the devices that are in range (approximately 50 meters) have visited, based on the algorithm described in section 3.1, as well as an overview of *open* networks these devices have in their network lists. The reason for this is that it is easy for people looking at this information to identify themselves (inviting them to further inspect the setup), while keeping privacy-sensitive information hidden from other people. Indeed, it is infeasible to identify the locations a particular person has visited by looking at the aggregate information. Similarly, while it is possible to view the aggregate SSID information about all devices in range, it is infeasible to determine the networks a specific device connected to. This also caters to possible legal issues: before we started with the study, we sought advice on possible legal issues and ensured we were allowed to show the information on the public display.

The smaller, private display initially shows the steps a visitor has to undertake in order to view the information his/her own smartphone is leaking. As soon as user consent is given (by connecting to a specific network or scanning a QR code), his/her information is displayed in a specific matter (see Figure 3), distinguishing between open (dangerous) networks and closed networks. Also displayed is the list of locations that SASQUATCH inferred to have been visited by the user.

After the participant information is displayed, he/she is asked to complete a short survey. The survey inquires on the accuracy of the displayed information, on how worried the user is about this information leaking to third parties, and on the amount of effort he/she would spend to mitigate information leakage. At the end of the study, the user is given a tutorial teaching him/her how to prevent future leaks.

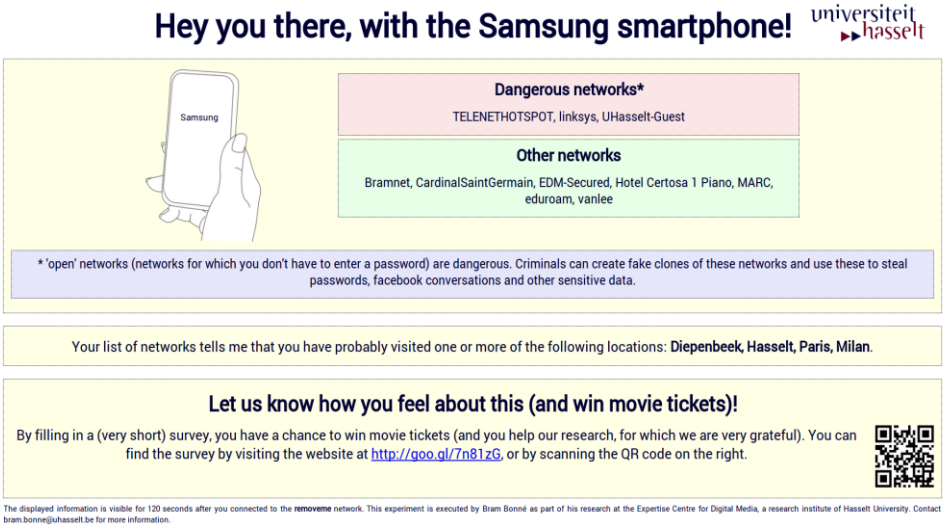

Fig. 3. A screenshot showing private information for a smartphone. Included are the lists of open and closed networks, the inferred locations, and an invitation to fill out the survey. Also briefly explained are the dangers of connecting to open networks.

5. RESULTS

During our field study, the setup captured Wi-Fi signals of 1404 devices. 82 people chose to show their personal data on the second screen of our setup, and 42 people filled out our survey. The survey participants (both male and female) were aged from 17 to 39 years old, all having completed high school or higher.

The packets sent out by smartphones during our study showed that the problem of a PNL containing open networks is widespread: of the 1404 devices that passed our setup, 628 (45%) contain at least one open network in their PNL. The second problem, where an eavesdropper would be able to determine a smartphone's whereabouts based on the networks in its PNL, is also real: we are able to relate 893 devices (64%) to at least one real-world location with a certainty of over 0.5 (calculated as in section 3.1). If we account for the fact that not everyone's full PNL was captured by only counting smartphones for which we captured at least 3 SSIDs, we find that of these 273 devices, 241 (88%) could be mapped to at least one real-world location.

To check the correctness of both the networks and the inferred location data, we asked the survey participants whether they were able to recognize their own data. 36 of the survey participants had chosen to display their data on the second screen, of which 63% indicated that nearly all or all information was correct, with the other 37% indicating that only part of the information was correct. This confirms our *first hypothesis*, which says that people are able to recognize their information when the data related to their smartphone is shown.

Survey participants were most surprised about an attacker's ability to spoof networks that were in their PNL: 23 of them (43%) expressed that they were not aware that this could be done. Furthermore, 22% of the participants was not aware their visited locations could be extracted by an eavesdropper, with 19% indicating they did not know their preferred networks could be seen by anyone with basic computer knowledge. In total, only 17% indicated that none of the displayed information surprised them, confirming our *second hypothesis* that most people are unaware about the data leaking from their smartphones.

90% of the surveyed people indicated that they were worried about someone being able to view the information we were able to gather. Survey participants were the least worried about the information leaking to friends, family or colleagues (16% of all participants), followed by civil authorities (20%), stores and marketing companies (23%), and other (random) people (31%).

Our *third hypothesis*, in which we state that people would be willing to put a minimal effort into making their smartphone more secure, is confirmed by the fact that 81% of the people surveyed indicated they were willing to make this effort, with 19% willing to do “whatever it takes”. When explicitly asked whether they were willing to install an app to mitigate the privacy and security issues discussed, 38% answered ‘yes’. 19% felt that it was the job of smartphone manufacturers to

secure their smartphones against these kinds of attacks, even if some of them indicated that they were willing to put in an extra effort to secure their smartphones themselves. Only four participants (6%) did not want to undertake action because they were not worried about information leakage from their smartphone. To cater to people willing to make their smartphone more secure, the end of the survey contained a link with instructions about how networks can be removed from a smartphone's PNL. As a result, we noticed that several of the participants removed one or more networks from their PNL after participating in our survey.

Interesting to note is that 60% of the people who filled in the survey wanted to be kept up-to-date on our new developments to help improve privacy and security for smartphone users: they actively ticked the box that their e-mail address could be used for further updates on this research.

6. SOLUTIONS

In this section, we describe some countermeasures that can be taken by either the smartphone user (short-term solutions) or by a smartphone manufacturer (long-term solutions) to protect against profiling of smartphone users by collecting their preferred networks, Evil Twin attacks, or both. As described in section 2, usability is an important factor to consider when increasing the security of a system [9]. For this reason, we aim to provide only solutions that have a minimal impact on user convenience and usability.

6.1. What the smartphone user can do

As a stopgap solution, users can largely secure themselves against profiling and Evil Twin attacks by removing networks from the PNL when they are not needed. While removing networks from the PNL is easy on both Android and Windows Phone mobile devices, iOS devices lack the capability of removing networks when they are not in range. Thus, iOS users wishing to remove networks from their PNL need to either be in range of the original network (which is often not possible), or need to actively spoof the network themselves when they want to remove it. Since our setup impersonates all networks requested by a smartphone, iOS users within Wi-Fi range of our setup are also able to remove these networks from their PNL. This solution, together with instructions on how to remove networks from a smartphone's PNL, was also displayed to users that finished our survey. We also included the remark that iOS users had the option of staying close to our setup in order to remove insecure networks from their list.

Similarly, iOS users are able to protect against the Evil Twin attack by enabling the option “Ask to Join Networks” in the Wi-Fi settings. Enabling this option will cause the iPhone or iPad to never automatically connect to a known network. Instead, it will ask the user for confirmation every time a network

connection is made, making this a typical trade-off between convenience and security.

Smartphone users can also secure their own managed networks (e.g. their home network) against the previously mentioned attacks by choosing a common SSID (e.g. `linksys` or `dlink`, which are among the highest ranking SSIDs in our dataset based on occurrence), and securing it with a non-common key. This effectively thwarts profiling by SSID because an eavesdropper has no way of knowing where the particular network the smartphone is referencing is located. Furthermore, Evil Twin attacks are prevented because an attacker has no way of knowing which key should be used when spoofing the network. Since this method requires the smartphone to have a common SSID in its network list, a disadvantage could be that the smartphone continually discovers networks it thinks are the home network of the user. This would lead the smartphone to try and fail to connect to each one of these networks, possibly draining the battery.

6.2. What a developer / manufacturer can do

A simple solution for preventing leakage of all SSIDs while providing the same existing convenience and ease-of-use to the user would be to not have the smartphone send out probe requests for known networks. However, this method is unlikely to be adopted by any major smartphone manufacturer, as it would require smartphones to continuously scan the Wi-Fi spectrum for beacons sent out by access points (known as ‘passive scanning’), necessitating the Wi-Fi radio to be enabled at all times.

A better option would be to use only *broadcast* probe requests. This type of probe request does not contain an SSID, and invites all access points in range to respond with a probe response containing the network identifier of the access point's network, enabling the smartphone to pick out its preferred networks. However, this approach would not work for networks with hidden SSIDs, as they require the client (in this case, the smartphone) to actively show its knowledge of the network beforehand. Lindqvist et al. [14] describe a privacy-preserving method for access point discovery allowing for the use of hidden access points using cryptography.

Limiting the broadcasting of probe requests would also mitigate the problem of connections that are being made to fake (Evil Twin) access points. Indeed, if no specific SSIDs are mentioned in probe requests, an adversary has no way of knowing which networks to spoof. However, an attacker will still be able to spoof generally available networks (e.g. McDonald's `Wayport_Access` network). To further protect against Evil Twin attacks, a smartphone could allow connections to a network only at locations where it is known to be in range (e.g. because the first connection was made at that location). Using the exact location, however, may cause the battery to drain at a faster rate because the smartphone's GPS is used. As

an alternative to using the exact location, connections to a network can be restricted to environments where a known set of other networks is also in range.

All of the previous solutions rely on smartphone manufacturers and smartphone OS builders to be universally implemented. However, operating systems like Android, Windows or GNU/Linux allow for applications to read and/or modify the Wi-Fi configuration, and to enable or disable networks in the PNL. This would allow for applications that either warn the user about forgotten access points (i.e. access points that have long not been used), that enable wireless networks on a per-location basis or that even only enable networks as soon as they are known to be in range (e.g. based on probe responses to broadcast probe requests). Disabling networks when not needed effectively stops the smartphone from sending out probe requests for these networks, mitigating both of the problems mentioned.

7. CONCLUSION

Similar to the security principle of *responsible disclosure*, our goal is twofold. First and foremost, we want to raise awareness on the data smartphones are leaking due to misconfiguration, insecure implementations or network protocol characteristics. Making users aware of this will encourage them to expect more from smartphone manufacturers with regard to handling privacy sensitive information in their smartphones, and will allow them to take action to make their smartphones more secure. Second, we show that possibilities exist for overcoming the discussed privacy and security issues at the level of the manufacturer, without having to make usability compromises.

We achieved the first part of our goal by having people interact with a public display setup that was designed to raise awareness. To stimulate people to look at our screen, we created a “honeypot effect” by having the display show open networks smartphones tried to connect to, as well as locations for all Wi-Fi networks smartphones were looking for. Once users started interacting with the public display more actively by scanning a QR code to indicate their interest in the matter, we informed them about ways in which they can improve privacy and security on their own smartphones.

We showed that smartphones leaking privacy sensitive information is a very real and common problem, and that a significant fraction of smartphone users are susceptible to the Evil Twin attack. Our study shows that 45% of users is in direct danger, and that 43% is not aware that such an attack was possible. Our approach to raise awareness on these issues was highly appreciated by the users (60% indicated they wanted to be kept up-to-date on our developments to help improve privacy and security for smartphone users) and has proven to be very effective for informing users (83% of users wasn't aware of these issues and is aware now).

ACKNOWLEDGEMENTS

We would like to thank some people who helped with the realization of this research: Kris Luyten for many original ideas behind this work; Bob Hagemann and the rest of the `WiGLE.net` team, for allowing the nearly unlimited use of their database; Pieter Robyns, for performance improvements to the spoofing code; and Arno Barzan and Jo Vermeulen for valuable feedback.

REFERENCES

[1] M. Cunche, M.-A. Kaafar, and R. Boreli, "Linking wireless devices using information contained in Wi-Fi probe requests," *Pervasive and Mobile Computing*, 2013.

[2] V. Roth, W. Polak, E. Rieffel, and T. Turner, "Simple and effective defense against evil twin access points," in *Proceedings of the First ACM Conference on Wireless Network Security*, ser. WiSec '08. ACM, 2008, pp. 220–235.

[3] B. Konings, F. Schaub, and M. Weber, "Who, how, and why? Enhancing privacy awareness in Ubiquitous Computing," in *PerCom Workshops*, 2013, pp. 364–367.

[4] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall, ""When I am on Wi-Fi, I am fearless": privacy concerns & practices in everyday Wi-Fi use," in *Proceedings of the 27th international conference on Human factors in computing* systems, ser. CHI '09. ACM, 2009, p. 1993.

[5] T. Kindberg, E. O'Neill, C. Bevan, V. Kostakos, D. Stanton Fraser, and T. Jay, "Measuring trust in wi-fi hotspots," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '08. ACM, 2008, pp. 173–182.

[6] J. L. Boyles, A. Smith, and M. Madden, "Privacy and data management on mobile devices," *Pew Internet & American Life Project*, September, 2012.

[7] O. Gunther and S. Spiekermann, "RFID and the Perception of Control: The Consumer's View," *Commun. ACM*, vol. 48, no. 9, pp. 73–76, Sep. 2005.

[8] S. Consolvo, J. Jung, B. Greenstein, P. Powledge, G. Maganis, and D. Avrahami, "The Wi-Fi privacy ticker: Improving awareness & control of personal information exposure on Wi-Fi," in *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, ser. Ubicomp '10. ACM, 2010, pp. 321–330.

[9] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *Proceedings of the 8th USENIX Security Symposium*, vol. 99. McGraw-Hill, 1999, p. 16.

[10] B. Bonné, A. Barzan, P. Quax, and W. Lamotte, "WiFiPi: Involuntary tracking of visitors at mass events," in *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*. IEEE, Jun. 2013, pp. 1–6.

[11] M. Marlinspike, "New tricks for defeating SSL in practice," *BlackHat DC*, February, 2009.

[12] H. Brignull and Y. Rogers, "Enticing people to interact with large public displays in public spaces," in *Proceedings of INTERACT*, vol. 3, 2003, pp. 17-24.

[13] B. Kowitz and L. Cranor, "Peripheral privacy notifications for wireless networks," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, ser. WPES '05. ACM, 2005, pp. 90–96.

[14] J. Lindqvist, T. Aura, G. Danezis, T. Koponen, A. Myllyniemi, J. Maki, and M. Roe, "Privacy-preserving 802.11 access-point discovery," in *Proceedings of the Second ACM Conference on Wireless Network Security*, ser. WiSec '09. ACM, 2009, pp. 123–130.

Information about the authors:

Bram Bonné – Bram is a PhD student in computer science at the Expertise Centre for Digital Media, a research institute of Hasselt University, where he specializes in computer security and privacy. He obtained MSc in Computer Science, specialization Software Security from KU Leuven in 2011.

Peter Quax – Peter Quax is an assistant professor at Hasselt University and a post-doc researcher at the Expertise Centre for Digital Media / iMinds. He obtained his MSc in Computer Science in 2000 and his PhD from the Transnationale Universiteit Limburg in 2007. His research interests are in networked virtual environments, on-line gaming, scalable multimedia delivery and security. He is a member of both ACM and IEEE.

Wim Lamotte – Prof. dr. Wim Lamotte obtained his MSc degree from the Free University of Brussels (1988) and a PhD in computer science (1994) at Hasselt University. He is a full professor at Hasselt University, where he leads the Multimedia Networking research group. Prof. Lamotte led and participated in numerous iMinds- and EU-funded projects on networked multimedia, mobile platforms and Quality of Experience. He is a member of the ACM (SIGCOMM and SIGMM) and IEEE (Computer Society and Communications Society).

Manuscript received on 15 July 2014

InfoTech-2015

Conference Proceedings Publishing and Dissemination

All accepted papers are reviewed by two independent reviewers for their scientific content and will be published in the PROCEEDINGS (ISSN 1314-1023) which will be deposited in the libraries listed below:

1. National Library "St. St. Cyril and Methodius", Sofia, ***Bulgaria***
2. NACID – Central Research and Technical Library, Sofia, ***Bulgaria***
3. Государственная публичная НТ библиотека (ГПНТБ), Moscow, ***Russia***
4. Всерусийский институт НТ информации (ВИНИТИ), Moscow, ***Russia***
5. Библиотека Росийской АН (РАН), Sanct Petersburg, ***Russia***
6. ГПНТБ Сибирскоко отделения РАН, Novosibirsk, ***Russia***
7. The Library of Congress, Washington, ***USA***
8. Technische Informationsbibliothek und Universitatsbibliothek, Hanover, ***Germany***
9. Universitatsbibliotthek, Stuttgart, ***Germany***
10. Universitatsbibliotthek, Kaiserslautern, ***Germany***
11. Centro de Informacion y Documentacion Cientifica (CINDOC), Madrid, ***Spain***
12. National Diet Library, Tokyo, ***Japan***
13. The Institution of Electronics and Telecommunication Engineers, New Delhi, ***India***
14. Biblioteca Stiintifica Centrala a Academiei de Stiinte, Chisinau, ***Republic of Moldova***

and

Libraries of Universities in Bulgaria, Czech Republic, New Zealand, Republic of Macedonia , Slovak Republic, etc.

The PROCEEDINGS of the International Conference on Information Technologies (InfoTech) is indexed by ***EBSCO Publishing Inc.,*** Ipswich, MA, **USA** (http://www.ebsco.com) and electronic version of the Conference PROCEEDINGS (e-PROCEEDINGS) will be included in three specialized scientific databases of ***EBSCO Host*** (http://www.ebscohost.com/title-lists)

- ***Academic Search Complete (Other Sources)***
  http://www.ebscohost.com/titleLists/a9h-other.htm
- ***Academic Search Elite (Other Sources)***
  http://www.ebscohost.com/titleLists/afh-other.htm
- ***Computers & Applied Sciences Complete (Database Coverage List)***
  http://www.ebscohost.com/titleLists/iih-coverage.htm