Raising Awareness on Smartphone Privacy Issues with SASQUATCH, and solving them with PrivacyPolice

Bram Bonné, Wim Lamotte, Peter Quax, Kris Luyten
iMinds/tUL/UHasselt
Wetenschapspark 2
3590 Diepenbeek, Belgium
{bram.bonne, wim.lamotte, peter.quax, kris.luyten}@uhasselt.be

ABSTRACT

Smartphones leak personal information about their owner when they use it to connect to the Internet. Despite recent coverage of these issues in popular media, raising awareness remains problematic since it remains largely invisible to the users. We designed a system, SASQUATCH, consisting of a network scanner and a public display, to draw the visitor's attention and inform them about these issues. SASQUATCH first gathers private information about previous whereabouts, and then shows an anonymized version of this data on the public display to draw the visitor's attention. Next, SASQUATCH offers an interactive component that allows people to view the information their own smartphone is leaking in private, and then provides solutions (including a fully-automated smartphone application) for securing against future privacy leaks. A set of initial field trails has shown that SASQUATCH is highly effective in raising awareness.

1. PROBLEM CONTEXT

Even though a significant amount of people carry a smartphone around all the time, most of them are unaware about the privacy impact of using such a device to connect to wireless networks. Indeed, studies have shown that the strategies which are currently used by mobile operating systems to search and connect to available wireless networks involve 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 [4]. 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 [10]. A study performed in 2009 by Klasnja et al. shows that users are unaware of the important privacy risks when using Wi-Fi networks [7]. 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.

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. [2] 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. Moreover, results presented by Consolvo et al. [3] show that a user's privacy awareness can be increased by showing the user personal information that is unwittingly shared.

Our work aims to inform smartphone users about the dangers of connecting to wireless networks, and to allow them to act in the interest of their own privacy. The first goal is accomplished by having a public display show privacy-sensitive information which is carefully abstracted and anonymized. The second goal is accomplished by providing a set of guidelines on how to prevent future privacy leaks, as well as by offering an Android application which automatically prevents leaking of sensitive information and avoids connections to impersonated wireless networks.

2. MOBILE PHONES "NEVER FORGET"

For long, mobile phones have been thought of as "trusted devices": they are used for private communication, coupled to a single user. In reality, smartphones are known to leak all kinds of data, caused in part by the the method that is used by most modern smartphones when scanning for known (or 'remembered') networks. This method is known as 'active scanning' and is implemented by having the smartphone actively send out the network names (SSIDs) of its preferred networks

Our initial field studies confirmed the findings of Klasnja et al. [7]; most people are not aware of this information leakage. In a first 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 names (*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 devices running iOS for example only show a stored network name when the network is in range, leaving users in the dark about which information is

MOBIQUITOUS 2014, December 02-05, London, Great Britain

DOI 10.4108/icst.mobiquitous.2014.258025

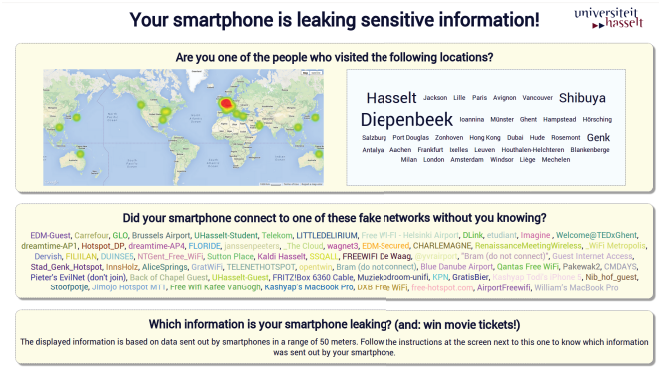

Figure 1: A screenshot of the public display. Top: the aggregate locations for all devices, together with a heat map of these locations. Bottom: a list of open networks devices tried to connect to.

leaking from their phones.

3. CREATING AWARENESS

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

1. 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, which allows to find the specific locations of access points. These locations are used to make an educated guess on the user's whereabouts.

2. The system executes an Evil Twin attack [10], impersonating networks in the smartphone's PNL, in order to identify which networks correspond to open access points.

3. 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[1].

The apparatus we deployed[2] for creating user awareness consists of two parts: a large display for public usage and a smaller one that can be used individually.

The public display (see Figure 1) is designed in a manner similar to work by Kowitz et al. [8], 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, as well as an overview of *open* networks these devices have in their network lists. This information is often sufficient for people to relate with and identify themselves, without the need to share more privacy sensitive information. This works as an attention grabber and pulls people to

[1]The OUI list is available at `http://standards.ieee.org/develop/regauth/oui/oui.txt`

[2]A video of our setup is available at `http://goo.gl/RClPf9`.

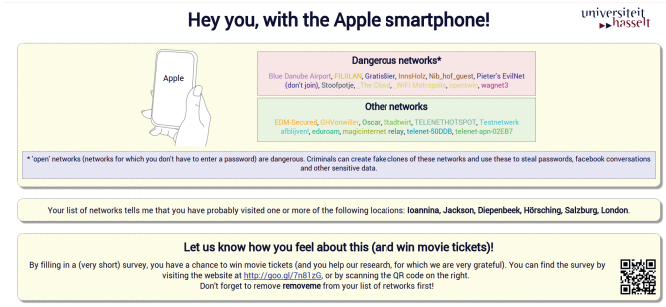

Figure 2: A screenshot of the private display. Included are the lists of open and secured networks and the inferred locations.

the screen. 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 these 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 2), distinguishing between open (dangerous) networks and secured networks. Also displayed is the list of locations that SASQUATCH inferred to have been visited by the user.

4. SOLVING PRIVACY ISSUES

In order to solve the privacy issues associated with mobile Wi-Fi usage in an automatic manner, we created a proof-of-concept Android application (called PrivacyPolice) preventing the attacks described before. We describe the functionality of the application in two parts: the prevention of network leaks, and the prevention of evil twin attacks. We tested both mitigation strategies on our personal devices for a period of 6 months, and using different types of wireless networks and access points. We noticed no degradation of the user experience.

4.1 Preventing network leakage

The leaking of SSIDs from the smartphone's PNL is prevented by using the application to disable all networks in the PNL by default. This prevents the 'active scanning method' described in section 1 from broadcasting directed probe requests. Instead, the application sends out a *broadcast* probe request, which does not contain any specific SSIDs, but requests all access points in range to respond with a probe response. If this results in a probe response being received for a network in the smartphone's PNL, the application reenables this network, allowing the smartphone to connect.

Broadcast probe requests are currently already used by smartphones to find networks that are not in the smartphone's PNL. They request all access points (instead of only access points corresponding to a single SSID) to reply with a probe response.

This approach does not work for networks that do not respond to broadcast probe requests, such as hidden (or

cloaked) networks. However, these types of networks are considered not to add any security, and the use of them has been discouraged for some time [5]. Apart from these exceptions, our experiments did not show any degradation of connection speed or quality.

4.2 Preventing evil twin attacks

Evil twin attacks are already partially mitigated by the strategy described in the previous section. Indeed, when this strategy is used, the attacker has no way of knowing which networks to spoof in order to have the victim connect to the evil twin access point.

However, an attacker could still try to spoof popular Wi-Fi networks, such as McDonald's `Wayport_Access` network in the US, or `BTWIFI` internationally[3]. If the popular network is in a victim's PNL, its smartphone will still automatically connect to the evil twin access point. To prevent this from happening, PrivacyPolice also remembers the MAC address of every access point in the smartphone's PNL. If the access point uses a MAC address that does not correspond to the MAC address of an access point previously connected to by the user (as might be the case when roaming), he/she is asked to explicitly confirm that the network is expected to be available at the current location.

This strategy does not completely prevent an attacker from mounting a successful attack: if the attacker is able to guess the exact access point the user has previously connected to, he/she can also spoof the access point's MAC address. However, this requires the attacker to have a priori knowledge about the victim.

4.3 Comparison to other mitigation strategies

In our previous journal paper, general solutions to the previous attacks (such as using a home network with a common SSID, but a unique key to thwart evil twin attacks) were already discussed [1]. Apart from these solutions, some other mitigation strategies have been proposed, ranging from improvements to the 802.11 discovery protocol [9] and MAC address randomization[4] to location-aware Wi-Fi probing [6].

While the first category of solutions requires modifications to the protocol, the second category is interesting because it allows users to protect themselves by installing an application (thus, without the cooperation of the smartphone vendor). There are, however, some differences between the proposed solutions and our own mitigation strategies.

First, location-based solutions require information from the GPS sensor. This makes it required for devices to have GPS enabled when scanning for wireless networks, which may be infeasible because of the battery impact, or because the device does not possess a GPS chip at all. Alternatively, the device could use the names of other networks in range in order to approximate its location. However, it is then easy to consider the case where a network is enabled only when the name for that network is in range, essentially corresponding to our own proposed method.

[3]A list of popular SSIDs can be found at `https://wigle.net/gps/gps/main/ssidstats`.

[4]Apple reported that, starting with iOS 8, iOS devices will randomize their MAC address when scanning for networks, as is explained in `http://devstreaming.apple.com/videos/wwdc/2014/715xx4loqo5can9/715/715_user_privacy_in_ios_and_os_x.pdf?dl=1`. This randomization is enabled only when both mobile data and location services are turned off.

Furthermore, similar to our method for preventing evil twin attacks, location-based solutions need to explicitly ask for the user's consent every time a new access point containing a known SSID is found, which may be less than satisfactory for networks that allow roaming, or when multiple access points provide access to the same network. This is insurmountable, and can be considered a policy decision. However, our solution allows the prevention of network leakage independent of the prevention of evil twin attacks, allowing the user to switch off the second functionality while still preserving his/her privacy.

5. FUTURE WORK

PrivacyPolice will be released as an app on Google Play. It will (if the user chooses to allow this) anonymously gather usage statistics, which can provide insights in how obtrusive the proposed approach is to a broader audience. Moreover, these statistics allow to gauge the app's usefulness to its users based on its retention rate.

6. REFERENCES

[1] B. Bonné, P. Quax, and W. Lamotte. Your mobile phone is a traitor! – Raising awareness on ubiquitous privacy issues with SASQUATCH. *International journal on information technologies & Security*, 6(3), Sept. 2014.

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

[3] 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 Ubicomp '10*, pages 321–330. ACM, 2010.

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

[5] J. Davies. Non-broadcast Wireless Networks with Microsoft Windows. *Microsoft TechNet*, Nov. 2005.

[6] Y. S. Kim, Y. Tian, L. T. Nguyen, and P. Tague. Poster: LAPWiN: Location-Aided Probing in Wi-Fi Networks. In *IEEE Symposium on Security & Privacy, San Francisco*, 2013.

[7] 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 CHI '09*, page 1993. ACM Press, 2009.

[8] B. Kowitz and L. Cranor. Peripheral privacy notifications for wireless networks. In *Proceedings of WPES '05*, pages 90–96. ACM, 2005.

[9] J. Lindqvist, T. Aura, G. Danezis, T. Koponen, A. Myllyniemi, J. Mäki, and M. Roe. Privacy-preserving 802.11 access-point discovery. In *Proceedings of WiSec '09*, pages 123–130. ACM, 2009.

[10] V. Roth, W. Polak, E. Rieffel, and T. Turner. Simple and effective defense against evil twin access points. In *Proceedings of WiSec '08*, pages 220–235. ACM, 2008.