Socio-technical Security Analysis of Wireless Hotspots

Ana Ferreira[1,2], Jean-Louis Huynen[1,2], Vincent Koenig[1,2], and Gabriele Lenzini[2,⋆]

[1] Institute of Cognitive Science and Assessment, Univ. of Luxembourg
[2] Interdisciplinary Centre for Security Reliability and Trust, Univ. of Luxembourg

Abstract. We present a socio-technical analysis of security of Hotspot and Hotspot 2.0. The analysis focuses is user-centric, and aim at understanding which user action can compromise security in presence of a attacker. We identify research questions about possible factors that may affect user's security decisions, and propose experiments to answer them.

Keywords: socio-technical security analysis, hotspot ceremonies.

1 Introduction

The increasing demand for WiFi Internet access is pushing several public spaces, such as hotels and airports, to offer Hotspots. These are open, unencrypted WiFi networks that may redirect mobile users to web sites where they have to pay a fee or accept some policy before being allowed to navigate the Internet. Hotspots are spreading fast for they are believed to be a solution to the overwhelming demand of high-bandwidth services which is presently saturating mobile networks. Unfortunately, current Hotspots offer little or no security [1][2], therefore Mobile Network Operators are hailing the newcomer Hotspot 2.0 [3]; this is expected to rely on a better technology[4], able to overcome present vulnerabilities by encrypting every interaction and isolating all client's sessions.

Hotspot 2.0 main functionalities are twofold: (1) the seamless roaming enables Mobile Network Operators to steer some traffic off the 3G and 4G networks to WiFi networks without user's intervention and (2) access points will be able to display information about their current load and available services before the user gains access to the network. The latter being surely useful for venues like a stadium facing very high demand in bandwidth due to some specific uses, like instant replays; the network could block unicast streaming traffic on the network and advertise the use of a multicast streaming service directly from the user's connection manager [5]. Hotspot 2.0 is thus advertised as a progress, with better security and better user experience.

However, despite its superior technical security, the *effective security* of this new technology will depend on how people will make use of it. This aspect is crucial as it has been proved that security mechanisms are rarely used by users

⋆ This research is supported by FNR Luxembourg, project I2R-APS-PFN-11STAS.

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 306–317, 2014.

as technically intended [6]. For instance, users may not trust Hotspot 2.0's new technology. Or users can accept it but the new acquired sense of security is no more justified if they switch back to conventional Hotspot, a situation that is possible since the old technology will continue to exist for some time, confusing users on what security risks can be present.

Analysing security issues with people in the loop demands for a *socio-technical* approach. This implies to look at the technical and the human protocols and to consider them together as complex layered ceremonies [7][8][9]. There is no such study for Hotspot and Hotspot 2.0, neither comparatively nor separately.

This paper covers this gap by describing Hotspot and Hotspot 2.0's most salient ceremonies and by studying their security with a user-centric approach. Its main goal is to raise future research questions and priorities about factors and mechanisms (e.g., user awareness, context, perception of security, trust) that may influence a more or less secure user behaviour in Hotspot's WiFi ceremonies. To devise those questions, we worked on four use-cases that cover most of the diversity of those ceremonies. In the next section, we first model the use-cases without any attacker (Section 3) and then perform a security analysis (Section 4). At the end of this paper (Section 5), we outline the setup of experiments allowing to answer the research questions that have emerged throughout this study.

2 Methods

The methods used to analyse socio-technical security of each use-case are: first we model the interaction between the different players of the ceremony with UML sequence diagrams; then we perform a security analysis by systematically devising the possible attacks when these interactions are exposed to threats according to a pre-defined threat model.

2.1 Modeling

We model ceremonies with UML sequence diagrams, a formalism that was successfully applied in socio-technical security analysis of TLS certificates [10]; it visually expresses all the sequential interactions (both Human-Computer and Computer-Computer) run by the players in the ceremony. This modelling is crucial for it defines the sets of interactions that can be analysed individually, in group, or at different levels of inter-dependency.

In order to get an objective analysis of the different use-cases, we divide the Hotspot ceremonies in common phases in which we identify one or more actions. Each action is the result of a decision, taken with or without user's involvement.

Prior is the action that happens before the user enters the ceremony; this is an optional pre-requisite (e.g., getting a SIM card by mail for instance); *Entry* is the entry point of the user, where he performs his initial action (e.g., open a url); *Selection* is the phase where the wireless network to be used is chosen from the list of available networks; *Access* is the action needed to successfully connect to the Hotspot (e.g., pay a fee); *Use* is where the user will actually use the network (e.g., performs again the action he tried in the *Entry* phase).

2.2 Security Analysis

Our analysis takes the user's point of view in the possible presence of an attacker who interferes with the user at *critical decision* points. These *critical decision* points are decision points from which the user can lose data confidentiality and integrity if the attack succeeds. For example, sending sensitive data should only take place when the WiFi is honest or the communication is encrypted. But, at this given *critical decision* point (choosing to send or not sensitive data on a communication channel), the attacker may push the user towards the unsafe behaviour, the *critical action* of sending the data. We first define the feasibility of the attacks through the following *threat model* and *assumptions*; then we identify the ceremonies' *critical actions* by assessing the user's risk in the security-analysis (Section 4).

Threat model: we consider two threats: (1) a Local Attacker (LA) that can read & write in the ether; it means in particular that it can bring up dishonest Access Points and listen to unencrypted messages; (2) a Distant Attacker (DA) that can read & write messages on the Internet; an attacker that provides a phishing link to the user falls in this category. LA and DA can also cooperate.

Assumptions: (1) we assume that all interactions taking place during the *Prior* phase are honest (2) we assume perfect encryption, meaning that the only way to decrypt encrypted information is by knowledge of the key. Under this assumption, HTTPS provides an unbreakable encryption and the honest server exposes a valid, verifiable certificate.

Risk assessment: the risk is described on a four-level scale: *null*, no attack is possible; *low*, the confidentiality or the integrity of user's action is threatened (e.g., when the attacker can listen to user's actions); *medium*, confidentiality of user's data threatened (e.g., when the attacker can listen to user's data); *high*, confidentiality and integrity of user's data threatened (e.g., when the attacker can tamper with the user's data).

Critical actions: are the actions for which the risk is at least medium, and also all other actions that are necessary for them to occur.

Results: we summarize the result of the analysis in tables. For each row – corresponding to a phase of the ceremony– we consider the following information in the columns: (1st) the *information* conveyed to the user, (2nd) the *actions* that the user can perform, (3rd) the *attacks associated* with this action, (4th) the *security property impacted* by these attacks, and (5th) a graphical representation of of the resulting *risk* level. The findings are further discussed in Section 5.

3 Use-Cases

We choose 4 use-cases that we think cover a large variety of situations. We concentrate on main differences like the automation (or lack of) the *selection* and *access* phases, the different types of players (e.g., persons, service providers), the need to pay during the *access* phase, the changes made to the encryption over time, and the information load and quality. We only consider a few types of authentication for the sake of space.

The first two use-cases relate to the Hotspot technology in use (abbreviated as HS1.1 and HS1.2) while the two last ones relate to the Hostpot technology users will encounter in the near future (abbreviated as HS2.1 and HS2.2).

HS1.1: Pay-Per-Use Hotspot. Fig. 1 shows the UML diagram for the pay-per-use ceremony of a typical captive portal Hotspot[1]. The players are a user, a browser, a connection manager, a wireless network provider and a payment platform. The *entry* point is a user who wants to browse the Internet; lacking of Internet connectivity, he proceeds to the *selection* phase where he scans for available networks and connects to the pay-per-use unencrypted wireless network. In the *access* phase, the user is redirected to the payment platform to pay the fee. The browser runs an HTTPS session, which often carries the usual HTTPS browser's cues (🔒), to execute the payment. After this step, the user is then free to *use* the (unencrypted) wireless network to browse the Internet.

HS1.2: Internet Service Provider's Homespot. This use-case is what is commonly called a Homespot. This is a residential router provided by an Internet Service Provider (ISP) that reserves most of its bandwidth for the customer who owns the device, but offers part of its capacity to the passer-by customers. The players are the (passing-by customer) user, his device's connection manager, the wireless network and the ISP. In the *prior* phase, the pre-requisites are that the user receives information (among these, the SSID) and his credentials. Using the same *entry* phase as HS1.1, the user then proceeds to the *selection* phase where he uses his connection manager to list the available Networks, and clicks on the one offered by the ISP. In the *access* phase, the browser is redirected to the ISP's online website, over HTTPS, where the user enters his credentials. As these are valid, the user gets a feedback from the webpage that he is now free to *use* the (unencrypted) wireless network

HS2.1: Mobile Network Operator's Partner Hotspot. Fig. 2 shows the UML diagram for the ceremony of a user connecting to a Hotspot 2.0 through his/her mobile phone. This requires no user interactions except the *entry* phase as the device will follow a pre-defined policy called ANDSF [11] to decide what network to join, and will use its SIM card to authenticate to the Hotspot. The ANDSF policy comprises user's preferences (e.g., always prefer user's home network), the Mobile Network Operator (MNO) preferences (e.g., roaming partners), the application requirements (e.g., steering traffic from VOIP to WiFi) and the Hotspot's conditions (e.g., the device should not switch to an overloaded Access Point). The pre-requisites (*prior* phase) are: the user gets the device pre-configured by his MNO, and sets some ANDSF preferences. The players are the user, the browser, an application, the connection manager, the wireless network and the MNO. In the *entry* phase the user opens a url in the browser which points to the content that requires the use of the application. The connection manager computes the policy bound to this application and concludes that it

[1] Captive portal : the user only has access to the Local Area Network until he pays a fee to be freed.

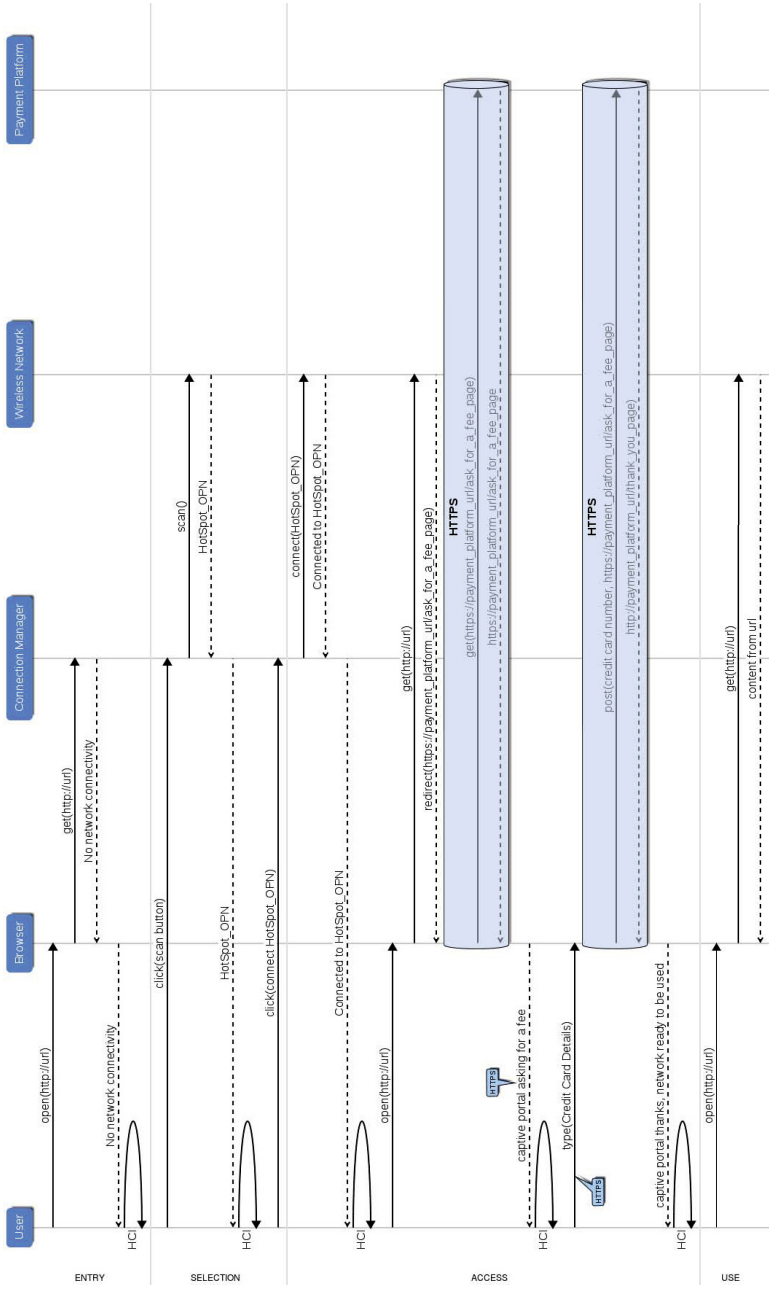

Fig. 1. UML diagram depicting user's interaction when joining a pay-per-use Hotspot. Components are at the top of each line, arrows represent exchanged messages: a plain line is used when a component initiates a message and a dotted line when a component replies to a message. The blue tunnels represent which messages are communicated within an encrypted tunnel with HTTPS.

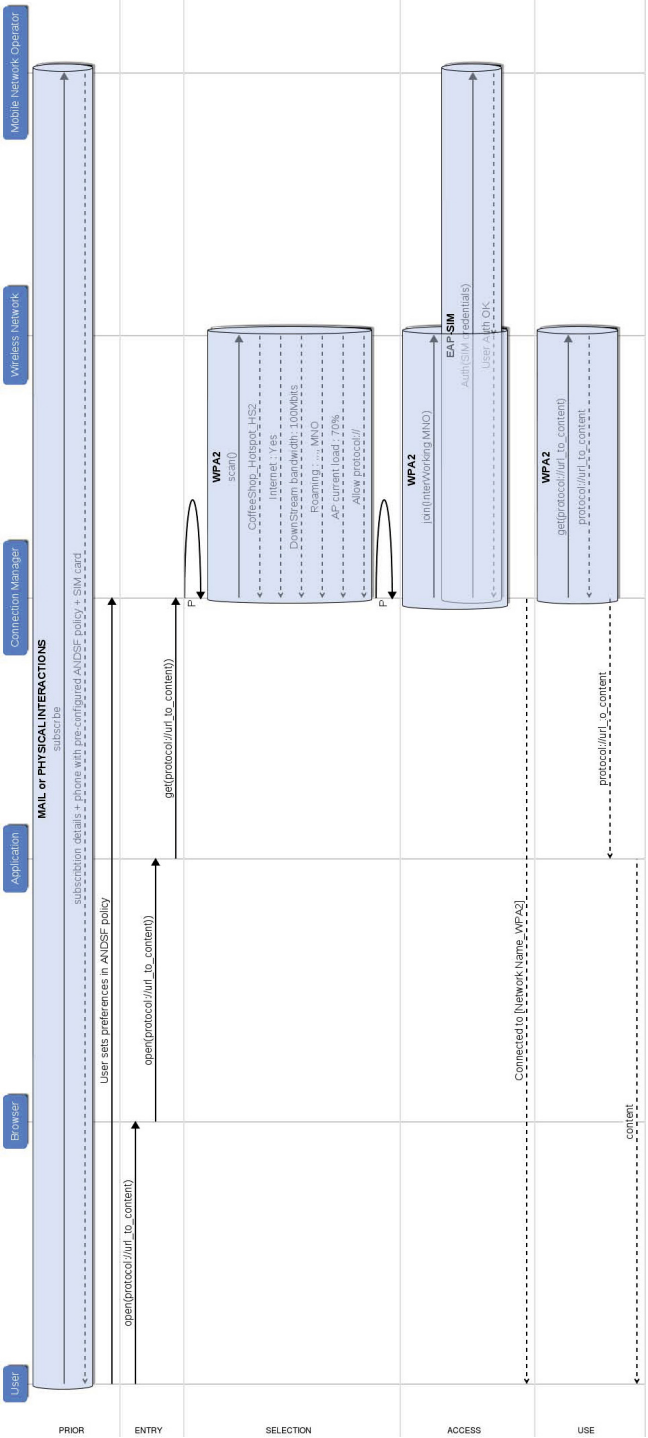

Fig. 2. UML diagram depicting user's interaction when Roaming on a Hotspot 2.0 Hotspot. Components are at the top of each line, arrows represent exchanged messages: a plain line is used when a component initiates a message and a dotted line when a component replies to a message. The blue tunnels represent which messages are encrypted using WPA2 protocol or communicated within an encrypted tunnel with HTTPS.

needs to connect to a WiFi wireless network. As a result, the connection manager automatically proceeds to the *selection* and *access* phases where it authenticates the user to the MNO. Once the connection is ready, the user is notified and, (*use* phase), the traffic corresponding to the content he requested is steered to the wireless network (encrypted with WPA2 Enterprise). Eventually this content is displayed to the user in the corresponding application.

HS2.2: The Future of Hotspots. This use-case focuses on the cohabitation of conventional Hotspots with Hotspot 2.0 with services support[2], when the automatic selection is disabled or impossible. The players are the user, the browser, the connection manager and the wireless network. The user's *entry* action is browsing the Internet; as there is no internet connectivity, he asks the connection manager to scan for available networks in the *selection* phase. The connection manager brings back results of: (1) conventional Hotspots with their SSID and signal strength; (2) Hotspot 2.0 networks with their SSID, signal strength, venue name, roaming partners, current load, WAN bandwidth, allowed ports; and eventually (3) services described by an icon and a url. The user then connects to one of the different candidates from the information at hand. Selecting (1) redirects the user to a use-case like HS1.1; selecting (2) or (3) sends the user to the *access* phase where the network automatically provisions him an account. As a consequence, all following interactions are encrypted with WPA2 Enterprise and the connection manager notifies the user that he joined the network. The *use* phase is different for (2) and (3): in (2) the user browses the Internet, in (3) the user's browser is redirected to the url specified by the service.

4 Socio-Technical Security Analysis

Our security analysis is user-centric, as such, its purpose is to pinpoint the critical actions prone to socio-technical attacks. Ultimately this leads to identifying upcoming research questions and possible laboratory experiments with users.

HS1.1: Pay-per-use Hotspot. Table 1 describes the security analysis of the HS1.1 use-case. In the first phase of interaction the user scans for open networks. As this interaction is not encrypted, it can be eavesdropped by a Local Attacker (LA) so, according to our risk assessment procedure described in Section 2, the risk is set as low. In the *selection* phase, the user picks a dishonest network from the list. By this action, the attacker only knows that his network has been picked; the risk is low. The *access* phase is protected by HTTPS, which by assumption sets the risk to null. In the last phase, *use*, the user decides now to use the network, here the user can give away a lot of possibly valuable information to an eavesdropper and the attacker can even tamper with subsequent actions if the user formerly selected the attacker's network, so the risk is high. The *selection* and *use* phases comprise *critical action* points and will be further discussed in Section 5.

[2] We assume the use of the existing CISCO's implementation of Hotspot 2.0 services, called MSAP; see chapter 12 of [12] for additional information.

Table 1. Socio-technical security analysis of the classic pay as you go captive portal

Phase	Information	Actions	Associated Attacks	Security properties impacted	Risk
Entry	No connectivity.	scan()	Eavesdropping scanning action.	Confidentiality.	
Selection	List of available networks.	connect(dishonest)	Eavesdropping picking action.	Authentication of the AP.	
Access	Webpage asking for a fee. HTTPS cues.	enter(credit card details)	-	-	
Use	Network ready.	open(url)	Eavesdropping information. Tampering.	Confidentiality. Integrity.	

HS1.2: Internet Service Provider's Homespot. In the Homespot use-case, the situation is closely related to HS1.1 as the user selects the attacker's network in the *selection* phase (again we set the risk as low). The attacker impersonates the ISP's wireless network but he can not (from assumption) tamper with the *access* phase, as the connection to the ISP relies on the HTTPS protocol (the risk is null). The attacker lets the user authenticate to the ISP, like he would do on a legitimate Homespot. In the *use* phase, the user takes the decision to browse the Internet on this connection, similar to the previous use-case. The risk is high as the user might lose confidentiality and integrity of his data. *Selection* and *use* comprise *critical* actions and will be discussed in Section 5.

HS2.1: Mobile Network Operator's Partner Hotspot. Table 2 describes the security analysis of this use-case. In the *prior* phase, setting a ANDSF policy does not pose any risk. In the *entry* phase, opening a url is considered as low risk because a DA can write a url in the Internet that, when clicked by the user, triggers the network discovery. The *selection* phase's actions are performed by the connection manager following the ANDSF policy (which has been altered by the user). The user can set a preference in the *prior* phase to rate unauthenticated, free Hotspot higher than the authenticated MNO's partners; this can be exploited by a LA which would provide a Hotspot 2.0 with corresponding characteristics. The risk would be high as the LA could eavesdrop and tamper with the user's data. LA and DA can also cooperate: LA can set an appealing hotspot while DA triggers network discovery. Both *critical actions*– setting a loose ANDSF policy and using a dishonest network–will be discussed in Section 5.

HS2.2: The Future of Hotspots. This use-case focuses on the *selection* phase when the automatic selection of an Hotspot is disabled. The user has to deal with different information emanating from different networks. The risk of connecting to a dishonest **network** that exposes appealing properties is high as it would

Table 2. Socio-technical security analysis of an automatic roaming to a Hotspot2.0 through an ANDSF policy

Phase	Information	Actions	Associated Attacks	Security properties impacted	Risk
Prior	SIM card. MNO information.	User sets its ANSDF preferences.	-	-	
Entry	url.	open(dishonnest url)	Trigger Network Discovery.	Authentication of source action.	
Selection	-	-	Appealing Hotspot2.0.	Authentication of AP.	
Access	-	-	-	-	
Use	Network Ready.	open(url)	Eavesdropping. Tampering.	Confidentiality. Data Integrity.	

lead the user to compromise his data's confidentiality and integrity in the last phase of the ceremony. The risk of selecting a dishonest **service** is even worse as the user would be automatically redirected to the url set by the LA. The factors that can influence this critical decision will be discussed in Section 5.

5 Discussion

For each *critical action* pointed out in the previous section, we elaborate on the following items: (a) research questions emerging from the *critical actions* about what factors (e.g., user's perception of security and trust, or user's awareness) affect the user's critical decisions; (b) experiments that need to be conducted to answer these questions.

HS1.1: Pay-per-use Hotspot
Selection phase: the user connects to a dishonest Hotspot As the only information conveyed to the user at this point is a list of available WiFi networks, the research question is: (a) what is the influence of the context, the signal strength and the likeliness of the name on the user's preferences? (b) In-vivo experiments based on deception (under strict compliance with ethical requirements like those of American Psychologists' Association - APA) followed by a survey are relevant to assess the importance of these different factors. Surveys and laboratory experiments where participants would have to choose from a network list to fulfil a high-stake task are relevant to refine our findings. Also, contrasting self-reported behaviour (surveys) with observed behaviour (e.g. lab experiments) would be useful to investigate users' awareness.

Use phase: the user uses a dishonest Hotspot As the user just pays a fee through an HTTPS connection before this *critical action*, we focus on the

perceived changes of the security properties. (a) Are users aware that security properties change over the course of this ceremony and that after a successful payment, subsequent ceremonies are done in an open/unencrypted connection? If users are aware, what is their degree of awareness and how does that affect their subsequent actions? If users are not aware, do they feel the same sense of security during the whole ceremony or does it change at different stages? Do they perceive the signal and cues that can trigger user awareness for the change? Is there any more adequate contextual information that could improve users' perception of this change? (b) The main challenge here is to investigate how HCI factors impact the awareness and responses to security properties. Laboratory experiments can be set up, e.g., using different security properties as different conditions ideally in a between subjects design. Comparing user behaviour across the conditions would provide strong indicators that could be further understood through interview techniques.

HS1.2: Internet Service Provider's Homespot
Use phase: the user uses a dishonest Homespot We focus here on the impact of an unauthenticated and authenticated interaction with the ISP. (a) Does impersonating an ISP tend to foster a trust relationship with the network? Does interacting with the ISP through a secured-connection foster a trust relationship with the network? Is this true for any player representing authority? (b) Those questions can be investigated with laboratory experiments: users would have to perform critical activities (e.g., e-banking) through different networks–some impersonating ISPs, some authenticated as ISPs. Comparing user behaviour across these different conditions provides indicators that could be further understood through interviewing techniques. One important aspect in these experiments consists in reliably simulating the "risk" without compromising ethical requirements.

HS2.1: Mobile Network Operator's partner Hotspot
Prior phase: the user sets a loose ANDSF policy This decision can be linked to economic considerations, as the MNOs will sign many roaming agreements with different partners, they may keep track of the amount of data consumed by their customers when roaming on WiFi network. If this roaming is not free, users will be tempted to prioritize roaming on free Hotspot whenever they can. (a) How much money are users ready to pay to use the safe roaming partners of their ISP? Are they aware that free Hotspot may be free for dishonest reasons? (b) A laboratory experiment where people would have to do a trade-off between security and money would be relevant to investigate further this question. This could be achieved through a setup where different test conditions require different fees to pay. An alternative approach could consist in having experiment participants match different usage scenarios with different MNO fees and free hotspots. Indeed, various approaches could be set up here or even combined.

Use phase: the user uses a dishonest Hotspot 2.0 The network is chosen automatically by the device (a) Are users aware of which policy rule lead them to use this network? Are users aware of the cost of such a use? Are users aware of the

modality of this connection (e.g., 3G/4G/WiFi)? Do users trust a connection after having been notified of its occurrence without having asked for it ? Do users trust their connection on their MNO's network through a third-party as much as a direct connection? What is the effect of the presence of a seam on the user's trust? (b) These usages are new and the technology supporting them is not widely available yet, therefore the experiments can not be easily built on existing "usage" standards. Interviews can be performed either in vivo or in a laboratory setup, with people who just experienced some of these situations, to understand what they are aware of in terms of security.

HS2.2: The future of Hotspots
Selection phase: the user connects to a dishonest Hotspot (a) Does adding more information about the networks help users to select honest WiFi networks? What is the phishing potential of those new information and services? Are users capable of searching for a network to fulfil a task and end up choosing a service instead? (b) Laboratory experiments where participants would have to choose a wireless network to fulfil a high-stake task are relevant to answer these questions. Networks would expose a range of technical qualities; services would be more or less appealing and related to the task.

6 Conclusion

This paper presents a detailed security analysis of hotspots. From this analysis, is possible to identify the various phases of a scenario where the user may affect security. It allows for a better understanding of how each phase may affect the security of subsequent phases or actions.

There is no one-size-fits-all solution. With the implementation of Hotspot2.0, we recommend that it needs to be better tested for socio-technical security. Although technical security has improved in comparison with the previous hotspot version, many issues still need addressing before its full deployment and usage in parallel with that previous version (which will not quickly disappear). We have provided a series of research questions and experiments to face some of the encountered security problems that industry and research will have to deal with.

There are also limitations to our work. The analysis was constrained by the specifications of the documentation that was available at the moment that is was performed. Event though Hotspot2.0 is considered superior with regard to security, our contribution shows such a system can be attacked and further research is needed. This on the other hand is made difficult by the relative lack of documentation on Hotspot2.0 at this stage. Moreover, our proposed research questions do not represent a comprehensive list and are rather a selection of questions we consider important to tackle next. There may be other relevant questions to address once we start answering the proposed ones.

We believe that it is important to analyse security of socio-technical systems, especially of hotspots, in this manner, because many technical attacks can only be fully successful at the user's end. The security analysis presented in this paper

can help us focus on understanding what makes a user fall or not for that attack and devise more appropriate defences.

References

1. Chenoweth, T., Minch, R., Tabor, S.: Wireless insecurity: examining user security behavior on public networks. Commun. ACM 53(2), 134–138 (2010)
2. Stakenburg, D., Crampton, J.: Underexposed risks of public wi-fi hotspots (2013), http://ComputerWeekly.Com (accessed April 23, 2014)
3. W.-F. Alliance. Wi-fi certified passpoint: A new program from the wi-fi alliance to enable seamless wi-fi access in hotspots (June 2012), http://www.wi-fi.org (accessed April 23, 2014)
4. 802.11u-2011–Amendment 9: Interworking with External Networks, IEEE Std., http://standards.ieee.org/findstds/standard/802.11u-2011.html (accessed April 23, 2014)
5. Brodkin, J.: Nfl to block mobile streaming video in super bowl stadium (January 2014), http://arstechnica.com/information-technology/2014/01/nfl-to-block-mobile-streaming-video-in-super-bowl-stadium (accessed April 23, 2014)
6. Klasnja, P., Consolvo, S., Jung, J., Greenstein, B.M., LeGrand, L., Powledge, P., Wetherall, D.: "When I am on Wi-Fi, I am Fearless": privacy concerns & practices in everyday wi-fi use. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI 2009, pp. 1993–2002. ACM, New York (2009)
7. Bella, G., Coles-Kemp, L.: Layered Analysis of Security Ceremonies. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) SEC 2012. IFIP AICT, vol. 376, pp. 273–286. Springer, Heidelberg (2012)
8. Ferreira, A., Huynen, J.-L., Koenig, V., Lenzini, G., Rivas, S.: Socio-technical study on the effect of trust and context when choosing wifi names. In: Accorsi, R., Ranise, S. (eds.) STM 2013. LNCS, vol. 8203, pp. 131–143. Springer, Heidelberg (2013)
9. Ferreira, A., Giustolisi, R., Huynen, J., Koenig, V., Lenzini, G.: Studies in Socio-Technical Security Analysis: Authentication of Identities with TLS Certificates. In: Proc. of the 12th IEEE TrustComm 2013, pp. 1553–1558 (2013)
10. Bella, G., Giustolisi, R., Lenzini, G.: Socio-Technical Formal Analysis of TLS Certificate Validation in Modern Browsers. In: Proc. of PST 2013. IFIP, pp. 309–316 (2013)
11. 3GPP Technical Specification 24;312 Access Network Discovery and Selection Function (ANDSF) Management Object (MO), 3GPP Std., Rev. 12.3.0 (December 2013), http://www.3gpp.org/DynaReport/24312.htm (accessed April 23, 2014)
12. Cisco, Cisco context-aware service configuration guide - 7.3, http://www.cisco.com/ (accessed April 23, 2014)