Wi-Trust: Improving Wi-Fi Hotspots Trustworthiness with Computational Trust Management

Seigneur, Jean-Marc

WI-TRUST: IMPROVING WI-FI HOTSPOTS TRUSTWORTHINESS WITH COMPUTATIONAL TRUST MANAGEMENT

Jean-Marc Seigneur

Réputaction SAS and CUI, Medi@LAB, ISS, Sociology Department, G3S, University of Geneva

ABSTRACT

In its list of top ten smartphone risks, the European Union Agency for Network and Information Security ranks Network Spoofing Attacks as number 6. In this paper, we present how we have validated different computational trust management techniques by means of implemented prototypes in real devices to mitigate malicious legacy Wi-Fi hotspots including spoofing attacks. Then we explain how some of these techniques could be more easily deployed on a large scale thanks to simply using the available extensions of Hotspot 2.0, which could potentially lead to a new standard to improve Wi-Fi networks trustworthiness.

***Keywords*—** Wi-Fi, public hotspot, computational trust

1. INTRODUCTION

The European Union Agency for Network and Information Security (ENISA) gives the following definition for Network Spoofing Attacks: "An attacker deploys a rogue network access point (Wi-Fi) and users connect to it. The attacker subsequently intercepts (or tampers with) the user communication to carry out further attacks such as phishing". This type of attack is ranked number 6 in its list of top ten smartphone risks [1]. In order to mitigate this risk, the Wi-Fi Alliance and Wireless Broadband Association have worked on a new standard called Hotspot 2.0 (HS 2.0) or Wi-Fi Certified Passpoint. Unfortunately, most hotspots currently deployed are legacy hotspots and it is going to take time and efforts to change them into Hotspot 2.0-enabled devices. In 2014, Ferreira et al. [2] underline regarding Hotspot 2.0 that "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)". In addition, even a Hotspot 2.0 may be compromised or controlled by an untrustworthy provider who can carry out different types of man-in-the-middle attacks if the user does not use a VPN. Therefore, authentication alone is not enough because the authenticated hotspot may be controlled by an untrustworthy owner/provider or attacker who has broken into the hotspot: another layer of trust is necessary on top of authentication trust to make the decision to use one or another available hotspot in user range.

Section 2 discusses what has been proposed so far to tackle remaining trust issues in hotspots, starting with computational trust management background and how it has been applied to hotspots by others and us. It also includes how we have validated it as part of different research projects [3]–[6] that we have carried out funded by the European Commission under the Seventh Framework Programme. In Section 3, based on this previous work that has shown the usefulness of computational trust for increased hotspot trustworthiness, we present our proposal for new standard for trustworthy hotspots selection and promotion called Wi-Trust that can be easily applied on top of Hotspot 2.0. Section 4 concludes with future work towards that standard.

2. COMPUTATIONAL TRUST TO MITIGATE REMAINING HOTSPOTS SECURITY HOLES

In this section, we first explain how computational trust based on the human notion of trust is different from the traditional concept of trust in computer security. Then, we detail the remaining security holes in Wi-Fi hotspots and the previous attempts to tackle these security holes both by others and us.

2.1. Computational Trust Management

In the human world, trust exists between two interacting entities and is very useful when there is uncertainty in result of the interaction. The requested entity uses the level of trust in the requesting entity as a mean to cope with uncertainty, to engage in an action in spite of the risk of a harmful outcome. There are many definitions of the human notion trust in a wide range of domains, with different approaches and methodologies: sociology, psychology, economics, pedagogy, etc. These definitions may even change when the application domain changes. However, it has been convincingly argued that these divergent trust definitions can fit together [7]. Romano's definition tries to encompass the previous work in all these domains: *"trust is a subjective assessment of another's influence in terms of the extent of one's perceptions about the quality and significance of another's impact over one's outcomes in a given situation, such that one's expectation of, openness to, and inclination toward such influence provide a sense of control over the potential outcomes of the situation"* [8].

Interactions with uncertain results between entities also happen in the online world. So, it would be useful to rely on trust in the online world as well. However, the terms trust, trusted, trustworthy and the like, which appear in the traditional computer security literature, have rarely been based on these comprehensive multi-disciplinary trust models and often correspond to an implicit element of trust – a limited view of the facetted human notion of trust. For

example, the trusted computing technology is assumed to be trusted once for all, full point.

To go beyond a fixed mandatory trust assumption, a computational model of trust based on social research was first proposed by Marsh [9]. In social research, there are three main types of trust: interpersonal trust, based on past interactions with the trustee; dispositional trust, provided by the trustor's general disposition towards trust, independently of the trustee; and system trust, provided by external means such as insurance or laws [7]. A trust metric consists of the different computations and communications, which are carried out by the trustor (and his/her network) to compute a trust value in the trustee. Trust evidence encompasses outcome observations, recommendations and reputation.

A very well-known attack, which is difficult to mitigate in open environments such as the Internet because allocating only one digital identity per person in the world is still difficult to achieve on a worldwide scale, is called the Sybil attack [10]. There is not yet a perfect trust metric that is Sybil attack resistant in all situations and without any constraints but for example we created the "*trust transfer*" [11] trust metric that is resistant to Sybil attacks if only positive recommendations are propagated.

The EU-funded SECURE project [11] represents a well-known example of a computational trust engine that uses evidence to compute trust values in entities and corresponds to dynamic evidence-based trust management systems. As depicted in Figure 1 below, the decision-making component can be called whenever a trusting decision has to be made. The Entity Recognition (ER) [11] module is used to recognize any entities and to deal with the requests from virtual identities. Relying on recognition rather than strong authentication, which means that the real-world identity of the user must be known, is also better from a privacy point of view because there is no mandatory required link to the real-world identity of the user if recognition is used rather than authentication.

It may happen that the trusting decision is not triggered by any requesting virtual identity, for example, if the user device would like to select the trustworthiest Wi-Fi hotspot in range in the list of nearby found hotspots. Usually, the decision-making of the trust engine uses two sub-components [11]:

- a trust module that can dynamically assess the trustworthiness of the requesting entity based on the trust evidence of any type stored in the evidence store;
- a risk module that can dynamically evaluate the risk involved in the interaction, again based on the available evidence in the evidence store.

A common decision-making policy is to choose (or suggest to the user) the action that would maintain the appropriate cost/benefit. In the background, the evidence manager component is in charge of gathering evidence (e.g., recommendations, comparisons between expected outcomes of the chosen actions and real outcomes, etc.) This evidence is used to update risk and trust evidence. Thus, trust and risk follow a managed life-cycle.

2.2. Hotspots Security and Remaining Threats

In a 2012 report [12], Cisco underlined the following remaining security holes in legacy Wi-Fi hotspots security that may lead to identity theft: legitimate hotspot spoofing, session hi-jacking or eavesdropping on unencrypted Wi-Fi. Common defense was to use 802.1X Port Access Control for robust mutual authentication. However, large-scale deployment was too tricky: "the most challenging part of deploying 802.1X involves installing and configuring client-side software and user credentials" [13]. Using a VPN on top of unencrypted communication solves eavesdropping, but most users do not have or know a VPN, and they even less want to spend time configuring it or pay for it since public Wi-Fi hotspot is more and more assumed to be free. The centralization of VPN servers is also not great from a privacy protection point of view. Private enterprise networks based on WPA2-Enterprise certification do not suffer from these attacks because they use IEEE 802.11i security and EAP authentication. Unfortunately, WPA2-Enterprise technology cannot be applied to legacy Wi-Fi hotspot networks because the access point's 802.1X port blocks all communications prior to authentication.

Due to the limitations of legacy Wi-Fi hotspots, the Wi-Fi Alliance started to work on Hotspot 2.0 and launched its first versions in 2012 in order to automate selecting Wi-Fi networks based on user preferences and network optimization, granting access to the network based upon credentials such as SIM cards, without user intervention, over-the-air encrypted transmissions with Certified WPA2-Enterprise.

Regarding worldwide user strong authentication that would ensure giving only one digital identity to any user, it is not realistic. So far, all initiatives to achieve it have not succeeded; a global PKI (Public Key Infrastructure) has been deemed not feasible. Social and federated logins [14],

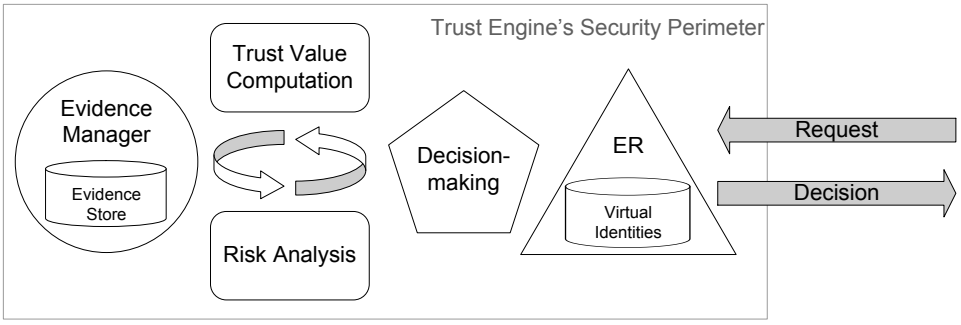

Figure 1. High-level View of a Computational Trust Engine

even though useful, cannot be tied properly to a real world identity because identities can be easily faked: for example, fake and zombie Facebook accounts are still a problem. Of course, if linking the user client with its real-world identity is done via strong authentication, the legal liability of the user client can be enforced but otherwise the hotspot sharer may be deemed liable in many countries. For example, in France, the Hadopi [15] law allows the French control service to use the IP address the Wi-Fi sharer to incriminate that Wi-Fi sharer if the user client cannot be strongly identified after having done illegal activities such as downloaded illegally shared copyrighted music.

On one hand, Hotspot 2.0 facilitates strong authentication of users linked to their real world identity because SIM-based authentication is possible. However, a SIM for a phone number may still not be linked to a real-world identity due to prepaid SIM whose owner real-world identity has not been verified yet. Filipinos services are known to provide fake Facebook accounts that have been validated with SIM. On the other hand, Hotspot 2.0 Release 2 is made to strongly authenticate the hotspot service provider. However, it does not mean that the owner of the authenticated hotspot is trustworthy. It may also happen that an attacker compromises a legitimate hotspot. Therefore even if user communication is encrypted between the user client and the hotspot or the hotspot service provider, the hotspot may have been compromised and man-in-the-middle attack is happening or the service provider itself may spy on unencrypted communication from the user. Another layer of trust is necessary on top of the authentication trust layer and computational trust is an appropriate means to compute that trust value in hotspots and service providers. With computational trust in the client user, even if the legal liability in the user is not enforced for sure, then the hotspot service provider can still allow access to trustworthy users and forbid access to untrustworthy ones.

2.3. Previous Attempts to Use Computational Trust in Hotspots

In this subsection, we first present the previous attempts to use computational trust in hotspots by others and then our own previous attempts.

Salem et al. [16] proposes a reputation system that enables the user to choose the best hotspot and discourages the Wireless Internet Service Providers (WISP) from providing a bad Quality of Service (QoS) to the mobile nodes. In their model, the behavior of each WISP is characterized by a reputation record, which is generated and signed by a trusted Central Authority (CA).

Momani et al. [17] introduce a new algorithm of trust formation in wireless sensor networks based on the QoS to be fulfilled by the network's nodes. They use three main sources to compute trust, namely direct observations (past experiences), recommendations from the surrounding nodes and fixed dispositional trust in nodes.

Trestian et al. [18] further examines network selection decision in wireless heterogeneous networks. They define a network reputation factor which reflects the network's previous behavior in assuring service guarantees to the user. Using the repeated Prisoner's Dilemma game, they model the user–network interaction as a cooperative game and show that by defining incentives for cooperation and disincentives against defecting on service guarantees, repeated interaction sustains cooperation. Their approach is very interesting because they focus on the user requirements or preferences although they do not prevent the user from connecting to malicious hotspots as we have done below.

As part of the FP7 EU-funded project called PERIMETER, we modeled and implemented a computational trust engine with a new trust metric called *TrustedHotspot* [3]. In our model, the behavior of each hotspot Access Point (AP) is characterized by a trust value in the range [0,1] computed based on the previous experiences of the users with that AP. Each AP owns its own private key and all messages are signed. We manage a central server hosting the cache of the trust values in each AP by each user. After using the AP, the user can rate it given different QoS rating possibilities. When possible, the QoS rating of the users are compared to automated technical measures such as average round-trips enforced by an additional application that must run on the user client. The user trust value decreases when it seems that the user has cheated when providing her/his rating. We have shown that it is more attack-resistant than Salem's one in [3].

We have also advanced computational trust management for hotspots in the other FP7 ULOOP project. First, we modeled and implemented an adaptive dispositional trust metric [19] where we don't use the dispositional trust level as a constant value as in Momani et al. [17] mentioned above, but as a value that can change over the time depending on the surrounding environment. Then, we have integrated trust management and cooperation incentives with our *"trust transfer"* trust metric [11], which has been proven to protect against Sybil attacks [10]. Our *"trust transfer"* trust metric implies that recommendations move some of the trustworthiness of the recommending entity to the trustworthiness of the trustee. Thus, in addition to assess trust, we can use the metric to reward in the form of trust points the agents that share their Wi-Fi connectivity [5]. To facilitate Wi-Fi sharing, we developed an Android app as part of the FP7 TEFIS smart ski resort project experimentation [20], which allowed locals to share their Wi-Fi network without taking the risk to be responsible of malicious activities done by the user client. Although it worked seamlessly for legacy personal hotspots and Android smartphones without having to jailbreak them, it is not yet possible to achieve the same level of automation with more controlled smartphones such as iPhones [6].

3. WI-TRUST: OUR NEW PROPOSAL TO PROMOTE TRUSTWORTHY HOTSPOTS

The above related work has shown the benefits of adding computational trust management to hotspots. It has also underlined that different authentication trust metrics as well as trust metrics in client users and hotspot owners exist. Unfortunately, previous work required too many changes in current Wi-Fi technologies to be easily deployable on a large scale. Therefore, our new proposal to reach wider

adoption should be able to easily plug different trust metrics. It is the reason we have based our proposal on the common high-level view of a computational trust engine as depicted in Figure 1.

In addition, to further facilitate worldwide adoption, it shouldn't require forcing too many changes in current hotspots standards. For example, Apple smartphones with iOS7 and Samsung S5, as well as Android M 6.0 and above, already supports some versions of Hotspot 2.0. Hence, we have investigated how to integrate our proposal with Hotspot 2.0.

Regarding the Entity Recognition (ER) component of a computational trust engine, fortunately, Hotspot 2.0 includes an Extensible Authentication Protocol (EAP) framework [21]. Therefore, we propose to map the ER module to this EAP part of Hotspot 2.0. Depending on the chosen authentication scheme selected between the client user and hotspot owner, then authentication trust can be computed. For example, SIM-based authentication is possible via EAP-SIM [22] and should get higher system trust than manual password-based only authentication. X509 certificates are also possible and the Wi-Fi Alliance has already allowed a few Certificate Authorities (CAs, e.g. Verizon, DigiCert and NetworkFX) to provide validated certificates for Wi-Fi hotspots providers to prove that their hotspot comes from a legitimate and trusted provider. In Hotspot 2.0 Release 2, a user client uses Online Sign-Up (OSU) to accomplish registration and credential provisioning to obtain secure network access. Each hotspot service provider has an OSU server, an Authentication Authorization and Accounting (AAA) server, and access to a CA, which is known by two attributes: its name and its public key. A user client trusts a hotspot if the OSU server has a certificate signed by a CA whose root certificate is issued by one of the CAs authorized by Wi-Fi Alliance, and that these trust root CA certificates are installed on the user client.

Since Release 1, Hotspot 2.0 has introduced new capabilities for automatic Wi-Fi network discovery, selection and 802.1X authentication based on the Access Network Query Protocol (ANQP), which forms the basis for 802.11u, an amendment to the IEEE 802.11 published in February 2011, and is a query and response protocol that defines services offered by an access point (AP), typically at a Wi-Fi hotspot. The ANQP communicates metadata useful for hotspot/AP selection process including the AP operator's domain name, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. When a subscriber queries an AP using the ANQP, that user receives a list of items that describe the services available, without having to commit to a network. In addition to the above-mentioned items, these elements can include geospatial and civic locations of the AP, capabilities of the network(s) being accessed, authentication types required by or available with the AP…

Thus, we propose to use those extra already available ANQP metadata fields called elements to exchange signed computational trust information in the hotspot at time of network selection by the user client. Different types of computational trust information are possible depending on the trust metric chosen but the main steps for exchanging computational trust information will follow the standard steps involved in the ANQP. Hence, our proposal to add computational trust management to hotspot is fully compatible with Hotspot 2.0 and can be seamlessly implemented in Hotspot 2.0 compatible hotspots by simply using the extra already available ANQP elements. For example, the OpenWrt [23] open source basis for hotspots, used by several hotspot providers such as FON, has already software components to be compatible with Hotspot 2.0. Figure 2 depicts the main sequence diagram of our proposal.

In Step 1, on the bottom left corner of the diagram, the user client, extended with our computational trust engine consisting of special hotspot selection policies and a potential additional installed app locally caching trust values, probes nearby hotspot to check whether or not they are compatible with Hotspot 2.0 and receives one from the nearby Hotspot 2.0 in the middle. In Step 2, the user client sends an ANPQ request including potentially Vendor Specific elements needed by the chosen and plugged computational trust metric used by the client. For example, our Sybil attack-resistant trust metric [11] or Salem's one [16]. In Step 3, the Hotspot 2.0 extended with our computational trust engine, initially implemented as an extension of OpenWrt Hotspot 2.0 implementation, checks the additional computational trust information sent in the ANPQ request elements and optionally gather during steps 4 and 5 other computational trust values in our new remote computational trust management (CTM) server. All trust values are signed by our CTM and can be passed back to the user client by the Hotspot 2.0 via ANPQ request answer Vendor Specific elements if needed. In Step 6, the user client receives the ANPQ request answer from the Hotspot 2.0 including optional Vendor Specific elements required by the trust metric. Locally cached and received computational trust values are used during step 7 by the user client to decide whether or not the Service Provider certified thanks to Hotspot 2.0 is trustworthy enough. Location coordinates of the Hotspot 2.0 may also be added in order to be able to trust not only the Service Provider owner of the Hotspot 2.0 but also the hotspot itself via the combination of location coordinates and Service Provider certification. If the user client decides to trust and select that Hotspot 2.0, the user client starts the normal Hotspot 2.0 authentication step with the Hotspot 2.0. In addition to carry out the normal authentication checks, the Hotspot 2.0 can optionally retrieve more trust information in the user client from the CTM server during steps 9 and 10 in order to decide during step 11 whether or not the user client is trustworthy enough to let it access the Internet through the Hotspot 2.0, for example, due to potential remaining legal liabilities of the hotspot owner when the user client accesses the Internet through the hotspot. If access is granted, then the user client accesses the Internet through the Hotspot 2.0 hotspot during Step 12 as usual. After its use, an optional step 13 is done by the user client to rate the QoS provided by the Hotspot 2.0 compared to what the Hotspot 2.0 proposed in the ANPQ answer. That new rating is turned into new trust evidence sent back to the CTM

server in step 14 and the CTM server updates the trust value in the Hotspot 2.0 during step 15. Based on the chosen and plugged trust metric, the new user client rating may be

In case of hotspots that are not easy to deploy according to Hotspot 2.0, such as personal hotspots shared by individuals because not everybody is able to manage extra

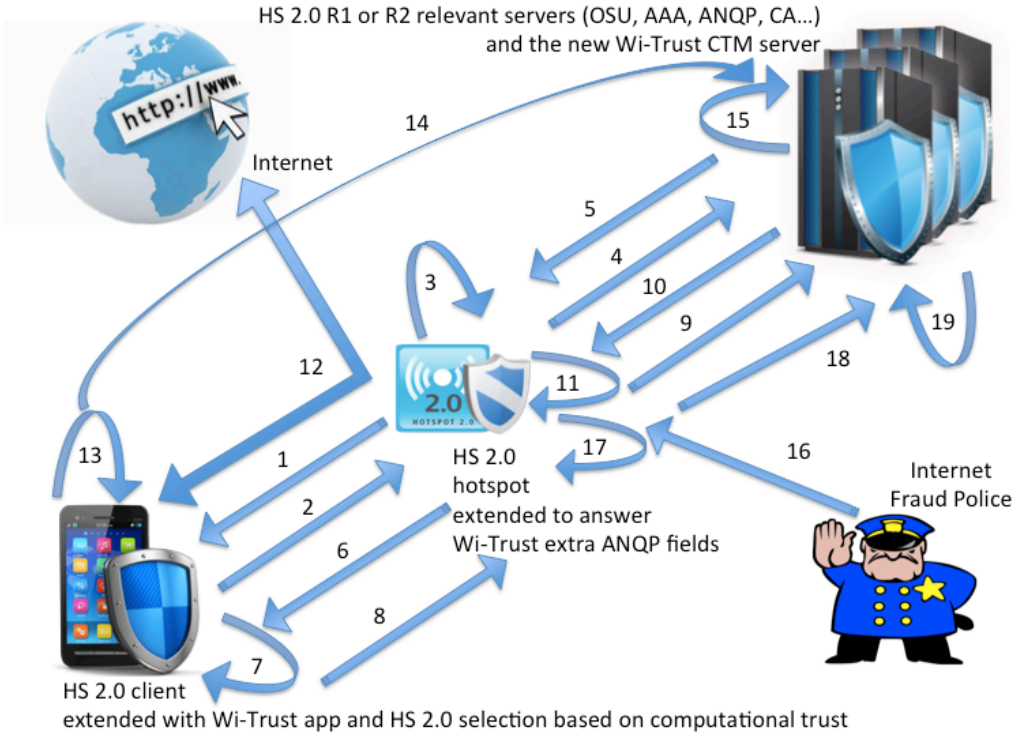

Figure 2. Wi-Trust Main Sequence Diagram

more or less trusted, for example, if the user client seems to consistently rate hotspots lower than others or other mechanisms are put in place to detect untrustworthy ratings as we demonstrated in [3]. Optionally, step 16 represents the case when an Internet fraud police institution, such as the French Hadopi institution created to monitor illegal Web activities by French users [15], contacts the Hotspot 2.0 owner due to illegal activity found at some stage from the Hotspot 2.0. In this case, the Hotspot 2.0 locally updates the trust value of the incriminated user client in step 17 and could inform the CTM server for further trust update on the server via steps 18 and 19.

Thus, thanks to our computational trust extension of Hotspot 2.0, 3 types of trust values can be computed:

1. Trust values in Wi-Fi service providers: these trust values will help selecting the most trustworthy service providers and encourage overall better Wi-Fi service quality because Wi-Fi providers will try to remain trustworthy in order to keep more users;
2. Trust values in Wi-Fi service providers hotspots: if location coordinates are used in addition to the certified service provider identity;
3. Trust values in user clients: user clients may be identified by various strong means depending on the EAP scheme used, for example, based on SIM number and trust values may concern their trustworthiness in rating service providers or not carrying out illegal activities such as downloading illegally shared copyrighted music.

servers such as Radius ones, although it may be possible to modify their software hotspot client and server to take into account trust values exchanged and stored in a similar way, worldwide adoption would be more difficult than with Hotspot 2.0, which is already backed up by major Wi-Fi stakeholders. The following table summarizes the available features.

Table 1. Available features

	Legacy Hotspot	Hotspot 2.0	Wi-Trust
Wi-Fi roaming authentication without initial manual intervention		*	*
Client/Hotspot encryption against eavesdropping		*	*
Strong authentication of the hotspot service provider and user client		*	*
Automated hotspot selection	*	*	*
Automated hotspot selection based on computational trust in hotspots and service providers			*
Hotspot owner legal liability mitigation by malicious user client exclusion based on computational trust			*

4. CONCLUSION

More and more users and devices want to use Wi-Fi to communicate and Wi-Fi may even be used to offload mobile data from telecom operator networks. Previous work has shown that computational trust management improves several security shortcomings of legacy hotspots but it was too difficult to deploy them on a large scale. We have presented how we could easily extend Hotspot 2.0 with computational trust management to even mitigate these shortcomings further. Legacy hotspots, which are likely to remain for a while, may also be extended with computational trust management, especially to secure collaborative Wi-Fi sharing with personal hotspots that cannot be achieved with Hotspot 2.0. However, there is much higher chance to achieve standardization of Wi-Trust based on Hotspot 2.0 because it doesn't require deep changes and can use open elements of Hotspot 2.0. We hope that our contribution published in the 2015 ITU Kaleidoscope conference will encourage standardizing Wi-Trust in a potential Hotspot 3.0 standard for increased trust in Wi-Fi.

5. ACKNOWLEDGEMENTS

The research leading to these results has received funding from the EU IST Seventh Framework Programme under grant agreement n° 224024, project PERIMETER (User-centric Paradigm for Seamless Mobility in Future Internet), under grant agreement n° 257418, project ULOOP (User-centric Wireless Local Loop) and under grant agreement n° 258142, project TEFIS (Testbed for Future Internet Services) smart ski resort experiment.

REFERENCES

[1] "Top Ten Smartphone Risks — ENISA." [Online]. Available: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks. [Accessed: 28-Jun-2015].

[2] A. Ferreira, J.-L. Huynen, V. Koenig, and G. Lenzini, "Socio-technical security analysis of wireless hotspots," in *Human Aspects of Information Security, Privacy, and Trust*, Springer, 2014, pp. 306–317.

[3] X. Titi, C. B. Lafuente, and J.-M. Seigneur, "Trust Management for Selecting Trustworthy Access Points," *IJCSI Int. J. Comput. Sci. Issues*, vol. 8, no. 2, pp. 22–31, 2011.

[4] J.-M. Seigneur, C. Ballester Lafuente, and A. Matos, "Secure user-friendly Wi-Fi access point joining," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, 2013, pp. 4718–4723.

[5] C. B. Lafuente and J.-M. Seigneur, "Extending Trust Management with Cooperation Incentives: Achieving Collaborative Wi-Fi Sharing Using Trust Transfer to Stimulate Cooperative Behaviours," in *Trust Management VIII*, J. Zhou, N. Gal-Oz, J. Zhang, and E. Gudes, Eds. Springer Berlin Heidelberg, 2014, pp. 157–172.

[6] C. Ballester Lafuente and J.-M. Seigneur, "Crowd Augmented Wireless Access," in *Proceedings of the 3rd Augmented Human International Conference*, New York, NY, USA, 2012, pp. 25:1–25:2.

[7] D. McKnight and N. L. Chervany, "The Meanings of Trust." MISRC 96-04, University of Minnesota, Management Informations Systems Research Center, 1996.

[8] D. M. Romano, "The Nature of Trust: Conceptual and Operational Clarification," Louisiana State University, PhD Thesis, 2003.

[9] S. Marsh, "Formalising Trust as a Computational Concept," Department of Mathematics and Computer Science, University of Stirling, RP 1994.

[10] J. R. Douceur, "The Sybil Attack." 2002.

[11] J.-M. Seigneur, "Trust, Security and Privacy in Global Computing," Trinity College Dublin, Ph.D. Thesis, 2005.

[12] Cisco, "The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular," 2012.

[13] L. Phifer, "Deploying 802.1X for WLANs: EAP Types." [Online]. Available: http://www.wi-fiplanet.com/tutorials/article.php/10724_3075481_2/Deploying-8021X-for-WLANs-EAP-Types.htm.

[14] T. El Maliki and J.-M. Seigneur, "A Survey of User-centric Identity Management Technologies," in *The International Conference on Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007*, 2007, pp. 12–17.

[15] S. Dejean, T. Pénard, and R. Suire, "Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français," *Publ. Rennes FR Univ. Rennes*, 2010.

[16] N. B. Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson, "Node Cooperation in Hybrid Ad Hoc Networks," *IEEE Trans Mob Comput*, vol. 5, no. 4, pp. 365–376, 2006.

[17] M. Momani, J. Agbinya, G. P. Navarrete, M. Akache, and others, "A New Algorithm of Trust Formation in Wireless Sensor Networks," in *The 1st IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless' 06)*, 2006.

[18] R. Trestian, O. Ormond, and G.-M. Muntean, "Reputation-based network selection mechanism using game theory," *Phys. Commun.*, vol. 4, no. 3, pp. 156–171, 2011.

[19] C. B. Lafuente and J.-M. Seigneur, "Dispositional Trust Adaptation in User-Centric Networks," in *Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on*, 2013, pp. 1121–1128.

[20] M. Yannuzzi, M. S. Siddiqui, A. Sällström, B. Pickering, R. Serral-Gracià, A. Martínez, W. Chen, S. Taylor, F. Benbadis, J. Leguay, J.-M. Seigneur, and others, "TEFIS: A single access point for conducting multifaceted experiments on heterogeneous test facilities," *Comput. Netw.*, vol. 63, pp. 147–172, 2014.

[21] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)." Network Working Group, 2004.

[22] H. Haverinen and J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)." [Online]. Available: https://tools.ietf.org/html/rfc4186. [Accessed: 12-Jul-2015].

[23] F. Fainelli, "The OpenWrt embedded development framework," in *Proceedings of the Free and Open Source Software Developers European Meeting*, 2008.