Wi-Trust: Computational Trust and Reputation Management for Stronger Hotspot 2.0 Security

J.-M. Seigneur

University of Geneva, Medi@LAB, G3S, CUI, Réputaction SAS
E-mail: jean-marc.seigneur@reputaction.com

Received 19 December 2016;
Accepted 8 March 2017

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 and reputation 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, reputation management.

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

Journal of ICT, Vol. 4_3, 213–236.
doi: 10.13052/jicts2245-800X.433

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 and reputation 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 a new standard for trustworthy hotspots selection and promotion called Wi-Trust that can be easily applied with Hotspot 2.0 extensions. Section 4 concludes with future work towards that standard.

2 Computational Trust and Reputation Management 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 and what is reputation management. 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 and Reputation 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.

Reputation is an old human notion: Romans named it "reputatio": "reputatio est vulgaris opinio ubi non est veritas." [10], which translates to reputation is a vulgar opinion where there is no truth. Reputation may be considered

as a social control mechanism [11], where it is better to tell the truth than to have the reputation to be a liar. That social control mechanism may have been challenged in the past by the fact that people could change of region to clear their reputation. However, as we move toward an information society world, changing of region should have less and less impact in this regard because reputation information is no more bound to a specific location, which is also a good news for reputable people who have to move to other regions for other reasons, such as a job relocation. For example, someone might want to know the reputation of a person that she or he does not know, especially when this person is considered to be chosen to carry out a risky task among a set of potential new collaborators. Another case may be that the reputation of a person is simply gossiped. The reputation information may be based on real, biased or faked facts, for example, faked by a malicious recommender who wants to harm the target person or biased by a recommender who is a close friend of the person to be recommended. The target of the reputation may also be an organization, a product, a brand or a location. The source of the reputation information may not be very clear, for example, it may come from gossips or rumors whose source is not exactly known or it may come from a known group of people. When the source is known, the term recommendation can be used. Reputation is different than a recommendation who is made by a known specific entity. The following gives an overview of the reputation primitives.

As La Rochefoucauld wrote[1] a long time ago, recommending is also a trusting behavior. It has not only an impact on the recommender's overall

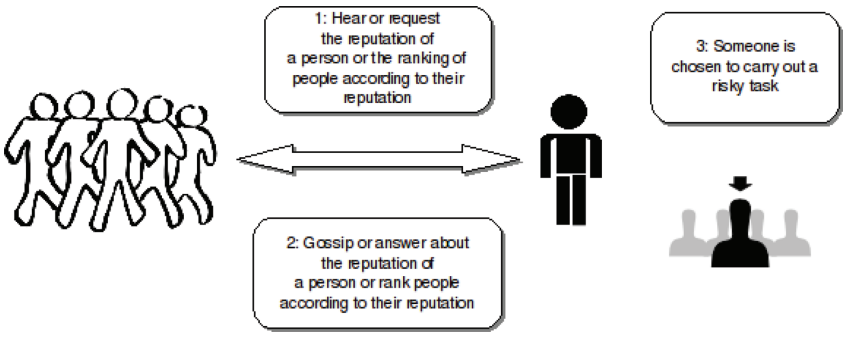

Figure 1 High-Level Reputation Primitives.

[1]Original quotation in French: La confiance ne nous laisse pas tant de liberté, ses règles sont plus étroites, elle demande plus de prudence et de retenue, et nous ne sommes pas toujours

trustworthiness (meaning it goes beyond recommending trustworthiness) but also on the overall level of trust in the network of the involved parties. La Rochefoucauld highlighted that when one recommends another, they should be aware that the outcome of their recommendation will reflect upon their trustworthiness and reputation since they are partly responsible for this outcome.

Benjamin Franklin noted about recommendations that each time he made a recommendation, his recommending trustworthiness was impacted: "in consequence of my crediting such recommendations, my own are out of credit" [12]. However, his letter underlines that still he had to make recommendations about not very well-known parties because they made the request and not making recommendations could have upset them. This is in line with Covey's "Emotional Bank Account" [13, 14], where any interaction modifies the amount of trust between the interacting parties and can be seen as favor or disfavor – deposit or withdrawal.

We define reputation as follows: "Reputation is the subjective aggregated value, as perceived by the requester, of the assessments by other people, who are not exactly identified, of some quality, character, characteristic or ability of a specific entity with whom the requester has never interacted with previously" [15].

To be able to perceive the reputation of an entity is only one aspect of reputation management. The other aspects of reputation management for an entity consist of:

- Monitoring the entity reputation as broadly as possible in a proactive way;
- Analyzing the sources spreading the entity reputation;
- Influencing the number and content of these sources to spread an improved reputation.

Therefore, reputation management involves some marketing and public relations actions. Reputation management may be applied to different types of entities: personal reputation management, which is also called personal branding or business reputation management. It is now common for businesses to employ full time staff to influence the company's reputation via the traditional media channels. Politicians and stars also make use of public relations services.

---

libres d'en disposer: il ne s'agit pas de nous uniquement, et nos intérêts sont mêlés d'ordinaire avec les intérêts des autres. Elle a besoin d'une grande justesse pour ne livrer pas nos amis en nous livrant nous-mêmes, et pour ne faire pas des présents de leur bien dans la vue d'augmenter le prix de ce que nous donnons.

For mass people, in the past, few media were available to easily retrieve people information, however as more and more people use the Web and leave digital traces, it now becomes possible to find information about any Web user via Google, which is known as googling someone. We have defined the following categories of online reputation services [15]:

Reputation Calculation: Based on evidence gathered by the service, the service either computes a value representing the reputation of a specific entity or simply presents the reputation information without ranking.

- Reputation Monitoring, Analysis and Warnings: The service monitors Web-based media (for example, Web sites, blogs, social networks or digitalized archived of paper-based press and trademarks) to detect any information impacting the entity reputation and warns the user in case of important changes.
- Reputation Influencing, Promotion and Rewards: The service takes actions to influence the perceived reputation of the entity. The service actively promotes the entity reputation, for example, by publishing Web pages carefully designed to reach a high rank in major search engines or paid online advertisements, such as, Google AdWords. Users reaching a higher reputation may gain other rewards than promotion, such as, discounts. Based on the monitoring services analysis, the service may be able to list the most important reputation sources and allow the users to influence these sources. For example, in a 2006 blog bribe case, it has been reported that free laptops preloaded with a new commercial operating system have been shipped for free to the most important bloggers in the field of consumer-oriented software in order to improve the reputation of the new operating software and the bloggers didn't mention that they had received the gifts.
- Interaction Facilitation and Follow-up: The service provides an environment to facilitate the interaction and its outcome between the trustor and the trustee. For example, eBay provides the online auction system to sellers and buyers as well as monitors the follow-up of the commercial transaction between the buyer and the seller.
- Reputation Certification and Assurance: That type of service is closer to the notion of system trust than the human notion of trust because it relies on externals means to avoid ending up in a harmful situation. For example, an insurance is paid as part of a commercial transaction. These services might need the certification of the link between the entity and its real-world identity in case of prosecutions.

- Fraud Protection, Mediation, Cleaning and Recovery: The above promotion services aim at improving the ranking of reputation information provided by the user rather than external information provided by third-parties. However, even if external information is hidden behind more controlled information, it can still be found. It is the reason that some services try to force the owners of the external sites hosting the damaging reputation information to delete the damaging information. Depending on where the server is located, it is more or less difficult to achieve. It may be as simple as filling an online form on the site hosting the defaming information to contact the technical support employee who will check if the information is really problematic. In the case of a reluctant administrator, lawyers or mediators specialized in online defamation laws have to be commissioned and it is more or less easy depending on the legislation in the country hosting the server. Generally, in countries with clear defamation laws, the administrators prefer deleting the information rather than going into a lengthy and costly legal process. Depending on the mediation and the degree of defamation, the host may have to add an apology in place of the defaming information, pay a fine or more. . . Fraud protection is also needed against reputation calculation attacks. There are different types of attacks that can be carried out to flaw reputation calculation results [16].

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 with multiple independent jurisdictions and countries, is called the Sybil attack [17]. 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" [18] trust metric that is resistant to Sybil attacks if only positive recommendations are propagated.

The EU-funded SECURE project [18] 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 2 below, the decision-making component can be called whenever a trusting decision has to be made. The Entity Recognition (ER) [18] 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

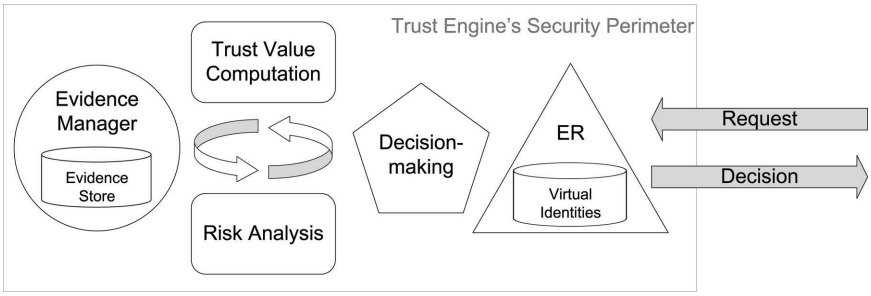

Figure 2 High-level view of a computational trust engine.

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 [18]:

- 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 Hotspot Security and Remaining Threats

In a 2012 report [19], Cisco underlined the following remaining security holes in legacy Wi-Fi hotspots security that may lead to identity theft: legitimate hotspot spoofing, session hijacking 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" [20]. 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 [21], 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 [22] 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.

2.3 Previous Attempts to Use Computational Trust and Reputation Management in Hotspots

In this subsection, we first present the previous attempts to use computational trust and reputation management in hotspots by others and then our own previous attempts. Salem et al. [23] 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. [24] 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. [25] 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. The users can become friends and have the possibility to ask to their friends for recommendations about a given AP. There is also the possibility to take into account the friend of friend recommendations based on a friendship factor. The recommendations are useful when the users have no information about an AP. In our system function (1), *nblink* defines the number of hops between two friends and it is likely to be inferior or equal to 6 according to the theory of the small world [26]. The result of this function is further used in the computation of the recommendation and it is implemented in our server. We have shown in [3] that it is more attack-resistant than Salem's one [23].

$$Friendshipfactor\ A \rightarrow B = \begin{cases} 1 & if\ A\ is\ a\ friend\ of\ B \\ \dfrac{2 + nblink}{2nblink + 1} & else \end{cases} \tag{1}$$

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 [27] where we don't use the dispositional trust level as a constant value as in Momani et al. [24] 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 [18], which has been proven to protect against Sybil attacks [17]. 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].

Based on the following Figure 3 below, Trust Transfer works in the following manner:

1. The subject requests an action, requiring a total amount of trustworthiness in the subject, in order for the request to be accepted by the trustor.
2. The trustor queries its contacts, in order to find recommenders willing to transfer some of their positive event outcomes count to the subject. Trustworthiness is based on event outcomes count in trust transfer.
3. If the contact has directly interacted with the subject and the contact's recommendation policy allows it to permit the trustor to transfer an amount of the recommender's trustworthiness to the subject, the contact agrees to recommend the subject. It queries the subject whether it agrees to lose some amount of trustworthiness on the recommender side.
4. The subject returns a signed statement, indicating whether it agrees or not.
5. The recommender sends back a signed recommendation to the trustor, indicating the trust value it is prepared to transfer to the subject. This message includes the signed agreement of the subject.

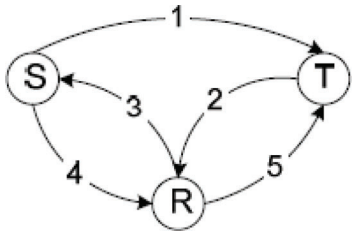

Figure 3 Trust transfer high-level view.

Trust Transfer can effectively be used as a cooperation incentive enabler, by using its trust points as the de facto "currency" in order to be able to use the services other users have to offer, in this case Wi-Fi connectivity sharing. By awarding trust points to the service provider proportionally to the duration of the Wi-Fi sharing period, we foster cooperation among users as not only the trust points reflect the good behaviour of the user giving her a good reputation, but also enable her to in turn obtain Wi-Fi connectivity when roaming or being out of data by using those trust points earned previously in order to pay for the service. The more you share in the system, and the more different users you share with, the easiest will be to in turn find another user which will accept your trust points as payment, be it because of having interacted directly with her or using trust transfer mechanisms to find another user who can lend the service requester those needed points. We reckon that these incentives are limited by the user's own circle of direct interactions and acquaintances inside the system, and this is why we exploit another capability of trust transfer, which is being able to transfer trust points through chains of trust with multiple hops. Finally, sharing may also happen thanks to our adaptive dispositional trust [27] and assuming that some users are disposed to trust even strangers unknown by their friends-of-friends.

To validate such peer-to-peer trustworthy Wi-Fi sharing, we developed an Android app as part of the FP7 TEFIS smart ski resort project experimentation [6, 28], 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 restricted smartphones such as iPhones whose access to some functionalities are restricted by Apple. As the deployment of dedicated public hotspots may be still too costly for small organizations such as small tourism boards or municipalities due to the fact that one hotspot only covers a small area and needs to be managed, our collaborative wireless access sharing between users is one step beyond the state-of-the-art. Simply put, local users to the environment become mobile hotspots on the fly, sharing their mobile data access, via their personal mobile hotspot in their device, with a foreigner for the (rather short or not) period of time that they might be in range. In this way, all the users that are either roaming or with no access to mobile data are still able to upload fundamental data and statistics and even use applications on places where normally they wouldn't be able to get connectivity through their own means or would be too expensive to do so. All of this, without having to deploy real fixed wireless access points and signal amplifiers, and

not limiting the area of coverage, as the access points are carried by the local people, which might be static or on the move.

Others have attempted to facilitate sharing data access with other users via Wi-Fi hotspots. To the difference of FON [29], which requires to have FON hotspot hardware, the Open Garden application [30] is software only (for Mac, Windows and Android only) and enables users to become part of a mesh network and access the most appropriate network without configuring their devices. Users can find the fastest connection and most powerful signal without checking every available network, and can move between networks seamlessly via Wi-Fi Direct or Bluetooth. However, Open Garden does not address the problem of the sharer being legally liable over the actions that any user connected to her or his Wi-Fi network might undertake. One of the biggest concerns with Wi-Fi access sharing is that all the data traffic goes out from the same source – the wireless router or access point – rendering the owner of the device liable in many countries such as France for any action that any user with whom she or he has shared the access with has performed, illegal content download, malicious actions taken against any entity or any other legally punishable action. This legal liability might deter many users from sharing their Wi-Fi or other type of data access, thus making it difficult for a service of this kind to succeed.

Open Garden aims for seamlessly connectivity without the intervention of the user. It doesn't strongly authenticate the clients or sharers and connections are made automatically without any initial configuration or authentication step. By default, there is no possibility to set any limit, thus no control over how much data is shared risking the danger of going over a certain monthly quota. By offering seamless connectivity between devices allowing easily the sharing of a Wi-Fi connection over 3G or 4G data, Open Garden effectively addresses the problem of high roaming costs, as foreign users can connect to other local users through their on the fly mesh network and obtain data access at no cost for them. Open Garden does not yet offer any incentive in the form of credits or rewards as we do. However, Open Garden plans to use some form of credits based on what can be seen on their Web site.

Air Mobs [31] is also an application that enables users to share their excess data with users who might be running up against their monthly limits. Essentially, one user agrees to let their mobile device act as a tethering hub that will send data from their LTE smartphone over Wi-Fi to any users nearby. In exchange, the central hub user gets a "data credit" that gives them access to other users' data in the future. Put another way, the new app creates a sort of "cap-and-trade" market for mobile data that helps users exceed the

hard limits set on their consumption by rationing data with one another based on their needs at given times. Air Mobs does not address the problem of the sharer being legally liable over the actions that any user connected to her or his Wi-Fi network might undertake. Air Mobs does not provide any means of strong authentication. Air Mobs monitors network connectivity and status in order to give the user the ability to control how much of her data plan she or he is willing to share, making sure other users cannot use more data than the amount designated by the owner of the hosting device. Air Mobs provides network connectivity when one device has no available Internet connection or roaming costs are too high, thus tackling effectively this problem. Air Mobs creates incentive via a secondary credit market – a user will be willing to share her or his data connection since she or he will get data in return.

In order to offer legal protection, being able to link the identity of the users with their real-world identities is of highest importance. As mentioned above, the Sybil attack [17] is one of the most concerning threats in trust and reputation systems, as it can subvert such a system completely if it is easy to create many fake identities. Regarding legal liability of the client or hotspot owner, in our proposed approach detailed in Section 3, we link social identities with real identities through credit card, when PayPal social login is used for example, or phone number verification enabled by Hotspot 2.0. Phone numbers not linked to a real identity are another threat to deal with, and can be mitigated by providing a period quarantine window, for example, 20 days, which is the maximum period of time a prepaid SIM card can be used in France without being linked to a real identity before being deactivated. Services that permit to acquire a disposable phone number such as Hushed [32] are dealt with, as in order to obtain one of these numbers a payment through a smartphone store or credit card is required, implying a link to the real-world identity if a police investigation is requested. Once linking the identity of strongly authenticated clients with real identities is done, their legal liability can be enforced by the fact that only their network communication signed with their private key can go through the hotspot and signatures are stored for proof in the future.

On one hand, Hotspot 2.0 will facilitate strong authentication of users linked to their real-world identity because SIM-based authentication will be possible. Of course, as written above, 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 [33]. On the other hand, Hotspot 2.0 is made to strongly authenticate the hotspot. However,

it does not mean that owner of the authenticated hotspot is trustworthy. Therefore, even if user communication is encrypted between user device and hotspot, the hotspot itself may spy on unencrypted communication from the user when it is in the hotspot. For example, in case of personal hotspots shared by users, it may be possible that the owner sharing the hotspot runs a modified version of the mobile device OS that allows her/him to eavesdrops the user communication. It may also happen that an attacker compromises a legitimate hotspot. 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. With computational trust in the client user, even if the legal liability in the user is not enforced for sure, then the hotspot owner can still allow access to trustworthy users and forbid access to untrustworthy ones.

3 Wi-Trust, our New Proposal to Easily Promote Trustworthy Wi-Fi Thanks To Hotspot 2.0 Extensions

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 [34]. 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 [35] 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 [36] open source basis for hotspots, used by several hotspot providers such as FON, has already software components to be compatible with Hotspot 2.0. The Figure 4 below depicts the main sequence diagram of our proposal.

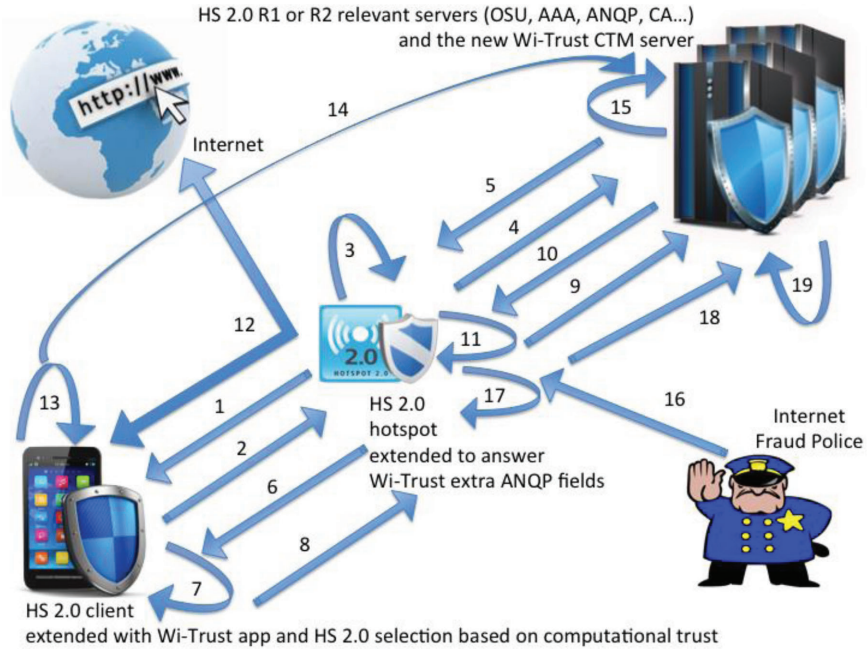

Figure 4 Wi-Trust main sequence diagram.

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 [18] or Salem's one [23].

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 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 [22], 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.

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 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 The available features are marked with an asterisk

	Legacy Hotspot	Hotspot 2.0	Wi-Trust	Open Garden	Air Mobs
Roaming (either with Wi-Fi or Wi-Fi direct) authentication without initial manual intervention		*	*	*	
Wi-Fi sharing incentives			*	*	*
Client/Hotspot encryption against eavesdropping		*	*	*	
Strong authentication of the hotspot service provider and user client		*	*		
Automated hotspot selection based on previously used hotspot (although unsecure)	*				
Automated hotspot selection based on computational trust in hotspots and service providers			*		
Hotspot owner legal liability mitigation by strong authentication linking the real-world identity of the user (e.g., via SIM card after quarantine period)		*	*		
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 and reputation 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 and reputation 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 initial 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. We have been invited to join the ITU Study Group 13 "Future networks including cloud computing, mobile and next-generation networks" Correspondence Group on Trust for this reason.

Acknowledgements

The research leading to these results has received funding from the EU IST Seventh Framework Programme under grant agreement no. 224024, project PERIMETER (User-centric Paradigm for Seamless Mobility in Future Internet), under grant agreement no. 257418, project ULOOP (User-centric Wireless Local Loop) and under grant agreement no. 258142, project TEFIS (Testbed for Future Internet Services) smart ski resort experiment.

References

[1] ENISA (2015). Top Ten Smartphone Risks – ENISA. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks [accessed June 28, 2015].

[2] Ferreira, A., Huynen, J.-L., Koenig, V., and Lenzini, G. (2014). "Socio-technical security analysis of wireless hotspots," in *Human Aspects*

of Information Security, Privacy, and Trust, eds T. Tryfonas, and I. Askoxylakis (Berlin: Springer), 306–317.

[3] Titi, X., Lafuente, C. B., and Seigneur, J.-M. (2011). Trust management for selecting trustworthy access points. *IJCSI Int. J. Comput. Sci*. 8, 22–31.

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

[5] Lafuente, C. B., and Seigneur, J.-M. (2014). "Extending trust management with cooperation incentives: achieving collaborative Wi-Fi sharing using trust transfer to stimulate cooperative behaviours," in *Trust Management VIII*, eds J. Zhou, N. Gal-Oz, J. Zhang, and E. Gudes (Berlin: Springer), 157–172.

[6] Lafuente, C. B., and Seigneur, J.-M. (2012). "Crowd augmented wireless access," in *Proceedings of the 3rd Augmented Human International Conference*, New York, NY, 25.

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

[8] Romano, D. M. (2003). *The Nature of Trust: Conceptual and Opera tional Clarification*. Ph.D. thesis, Louisiana State University, Baton Rouge, LA.

[9] Marsh, S. (1994). *Formalising Trust as a Computational Concept*. University of Stirling, Stirling.

[10] Bouvier, M. (1856). "Maxims of Law," in *Law dictionary*.

[11] Kuwabara, K. (2003). "Reputation: Signals or incentives?," presented at the The annual meeting of the american sociological association,

[12] Franklin, B., *The Life and Letters of Benjamin Franklin*. Milwaukee, WI: E.M. Hale & Company.

[13] Covey, S. R. (1989). *The 7 Habits of Highly Effective People*. Salt Lake City, UT: Franklin Covey.

[14] Seigneur, J.-M., Abendroth, J., and Jensen, C. D. (2002). "Bank accounting and ubiquitous brokering of trustos," in *Proceedings of the 7th Cabernet Radicals Workshop*, Bertinoro.

[15] Seigneur, J.-M. (2013). "Online e-reputation management services," in *Computer and Information Security Handbook*, 2nd edn, (Burlington, MA: Morgan Kaufmann).

[16] ENISA (2016). *Reputation-Based Systems: A Security Analysis –ENISA*. Available at: https://www.enisa.europa.eu/publications/archive/reputation-based-systems-a-security-analysis [accessed March 23, 2016].
[17] Douceur, J. R., (2002). "The sybil attack," in *Proceedings of the International Workshop on Peer-to-Peer Systems*, Cambridge, 251–260.
[18] Seigneur, J.-M. (2005). *Trust, Security and Privacy in Global Computing*. Ph.D. thesis, Trinity College Dublin, Dublin.
[19] CISCO (2012). *The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular*. San Jose, CA: CISCO.
[20] Phifer, L. (2003). *Deploying 802.1X for WLANs: EAP Types*. Available at: http://www.wi-fiplanet.com/tutorials/article.php/10724_3075481_2/Deploying-8021X-for-WLANs-EAP-Types.htm
[21] El Maliki, T., and Seigneur, J.-M. (2007). "A Survey of User-centric Identity Management Technologies," in *Proceedings of the The International Conference on Emerging Security Information, Systems, and Technologies*, (Norwood, SA: SecureWare), 12–17.
[22] Dejean, S., Pénard, T., and Suire, R. (2010). *Une Première Évaluation des Effets de la loi Hadopi sur les Pratiques des Internautes français*. Rennes: University of Rennes 1.
[23] Salem, N. B., Buttyán, L., Hubaux, J.-P., and Jakobsson, M. (2006). Node Cooperation in Hybrid Ad Hoc Networks. *IEEE Trans. Mob. Comput*. 5, 365–376.
[24] Momani, M., Agbinya, J., Navarrete, G. P., and Akache, M. (2006). "A new algorithm of trust formation in wireless sensor networks," in *Proceedings of the 1st IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless' 06)*, Sydney. NSW.
[25] Trestian, R., Ormond, O., and Muntean, G.-M. (2011). Reputation-based network selection mechanism using game theory. *Phys. Commun*. 4, 156–171.
[26] Gray, E., Seigneur, J.-M., Chen, Y., and Jensen, C. D. (2003). "Trust propagation in small worlds," in *Proceedings of the First International Conference on Trust Management*, Heraklion.
[27] Lafuente, C. B., and Seigneur, J.-M. (2013). "Dispositional trust adaptation in user-centric networks," in *Proceedings of the The 27th IEEE International Conference on Advanced Information Networking and Applications (AINA-2013),* Barcelona, 1121–1128.
[28] Yannuzzi, M., Siddiqui, M. S., Sällström, A., Pickering, B., Serral-Gracià, R., Martínez, A., et al. (2014). TEFIS: a single access point for

conducting multifaceted experiments on heterogeneous test facilities. *Comput. Netw*. 63, 147–172.
[29] FON (2016). *The World's Leading Carrier WiFi Provider*. Available at: http://www.fon.com [accessed February 09, 2016].
[30] Open Garden (2016). *Open Garden*. Available: https://opengarden.com/ [accessed February 09, 2016].
[31] AirMobs (2016). *AirMobs*. Available at: https://play.google.com/store/apps/details?id=org.eeiiaa.airmobs&hl=en [accessed September 02, 2016].
[32] Hushed (2016). *Talk and Message. . . Quietly*. Available at: http://www.hushed.com [accessed September 2, 2016].
[33] Doug Bock Clark (2015). *Inside a Counterfeit Facebook Farm*. Available at: http://theweek.com/articles/560046/inside-counterfeit-facebook-farm [accessed September 02, 2016].
[34] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and Levkowetz, H. (2004). *Extensible Authentication Protocol (EAP)*. Network Working Group, RFC 3748.
[35] Haverinen, H., and Salowey, J. (2015). *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*. Available at: https://tools.ietf.org/html/rfc4186 [accessed July 12, 2015].
[36] Fainelli, F. (2008). "The OpenWrt embedded development framework," in *Proceedings of the Free and Open Source Software Developers European Meeting* (Brussels: FOSDEM).

Biography

Dr. Jean-Marc Seigneur has published more than 100 scientific publications worldwide in the field of online reputation, trust, security and privacy. He is an expert of the European Network and Information Security Agency (ENISA), expert evaluator of the European Commission R&D multimillion euros'

projects and academic member of the ITU standardization efforts for security, trust and privacy in smart cities, Internet of Things (IoT) and converging networks. In 2010, he has launched the Augmented Human International Conferences series with now more than 1600 newsletter subscribers. After being a Research Fellow of Trinity College Dublin, he is now part-time Senior Lecturer & Research Manager at the University of Geneva, President of Réputaction SAS and Chief Marketing & Research Officer of GLOBCOIN at OPTIM INVEST SA. He has provided computational trust and online reputation management consulting to many companies (Amazon, Philips, Swissquote . . .) and has been on the scientific board of a few of them (Venyo, Thales . . .).