A User-centric Approach to Trust Management in Wi-Fi Networks

Carlos Ballester (University of Geneva), Jean-Marc Seigneur (University of Geneva), Paolo di Francesco (Level7), Valentin Moreno (FON), Rute Sofia (SITILabs, University Lusófona), Waldir Moreira (SITILabs, University Lusófona), Alessandro Bogliolo (University of Urbino), Nuno Martins (Caixa Mágica Software)

Abstract—This technological demonstration goes over a new trust management framework which can assist in achieving secure connections in wireless networks, without necessarily implying the use of strong security associations. The demonstration is based on open-source software, and has been developed to run on OpenWRT as well as on Android.

I. INTRODUCTION

The EU ULOOP project [1] is investigating and implementing technology to overcome the limitation of today's broadband access technologies, expanding the backbone infrastructure by means of low-cost wireless technologies that embody a multi-operator model, i.e., a local-loop based upon what a specific community of individuals (end-users) is willing to share, backed up by specific cooperation incentives and "good behaviour" rules. This represents a paradigm shift in the Internet evolution, as the user may be in control of parts of the network, in a way that is acknowledged (or not) by Internet stakeholders. In such scenarios where several strangers are expected to interact for the sake of robust data transmission, trust is of vital importance as it establishes a way for the nodes involved in the system to communicate with each other in a safe manner, to share services and information, and above all, to form communities that assist in sustaining robust connectivity models.

This technological demonstration goes over the trust management framework provided in ULOOP, which has been currently developed to run both in open-source Access Points (OpenWRT) and in Android. The demo shall assist in explaining how ULOOP envisions trust management to achieve security in a flexible way, without necessarily implying the use of strong security associations.

II. TRUST MANAGEMENT IN ULOOP

In ULOOP, trust management and cooperation incentives are related to the understanding of how to define and build circles of trust on-the-fly. Such circles of trust aim of sustaining an environment for allowing devices to share resources to support the dynamic behavior of user-centric networks. Trust management is based on reputation mechanisms able to identify end-user misbehavior and to address social aspects, e.g., the different levels of trust users may have in different communities (e.g., family, affiliation). In situations where the created network of trust is not enough to allow resources to be shared, ULOOP devices are able to use a cooperation incentive scheme that allows a node to gain credits in an amount directly proportional to the amount of shared resources: such credits

can then be used to gain access to other resources. Hence, trust management and cooperation incentives aspects are split into three main blocks: i) Trust management; ii) Cooperation Incentives; iii) Identity management.

From a ULOOP software suite perspective and as has been explained [2], there are modules which are activated if a ULOOP element plays the role of a regular *node*, or of a *gateway*. A *ULOOP gateway* is a role (software functionality) that reflects an operational behavior making a ULOOP node capable of acting as a mediator between ULOOP systems and non-ULOOK systems – the outside world. This gateway role may or may not be owned and controlled by a ULOOP user, it may also be controlled by an access operator. The key differentiating factor of the role of gateway, in contrast to a regular ULOOP node, is the operational intelligence and mediation capability. Similarly to ULOOP nodes, the ULOOP gateway functionality may reside in the user-equipment, in Access Points, or even in the access network. Hence, they exhibit a feature that is key in user-centric environments: their behavior as part of the network is expected to be highly variable. Gateways will be active or inactive based on several conditions such as users' wishes and network load. Then, and from a trust perspective, ULOOP considers the role of a *requestee* (providing resources) or of a *requester* (requesting access to a set of resources, such as Internet connectivity). A requestee in ULOOP can only be a ULOOP gateway. While the requester role can be assumed by both a node and a gateway: nodes perform trust negotiation towards gateways; gateways perform trust negotiation among themselves.

The trust management framework of ULOOP considers three distinct phases: i) setup; ii) activation of periodic activities - cooperation and rewarding; iii) data transfer, which are briefly explained next.

A. Trust Setup

The setup phase is executed in any ULOOP node, be it a requestee or a requester, since it aims to establish the initial set of conditions for the participation in a ULOOP community. A first step in this setup is the background creation of a virtual identity associated to the user (of n devices), the *crypto-id*. The *crypto-id* is used to assist the process of computing and managing the set of trust associations among any pair of ULOOP devices. The goal is to mitigate the impact of impersonation and non-repudiation, while insuring the right level of privacy. Hence, a *crypto-id* identifies a unique interconnection of a user and a device.

When a node joins ULOOP for the first time, a crypto-id (public-private key pair) is generated. After that the user can request a ULOOP partner (Identity Validator) the validation of such crypto-id, so that the end-user can prove with cryptographic strength that he/she really owns the secret linked to the crypto-id. Then, a next step in the setup is for the user to set its global willingness to trust others, parameter which we name as *dispositional trust (DT)*. If the user has multiple devices, he/she only has to set his/her dispositional trust for one device: the others will get that information from the first one when in direct contact. For the first device, the owner is prompted to set its DT, e.g. being able to select from a list of predefined values, which range from 0 to 1, being 0 “paranoid”, which means that a priori the node will not trust anyone, and being 1 “blind trust”, which means that the node will trust no matter what. If the device is not the first one being configured, the user is presented with two options: i) to clone the dispositional trust level assigned to other devices that are already in ULOOP and that she/he owns; ii) to assign a new DT level for the node being introduced.

At this stage, the ULOOP device has no trust level in the system and its trust on others (as given by the dispositional trust) may prevent such node from interacting with others. Thus, to overcome such issue, a certain amount of initial credits are assigned to the node. This will motivate the user to interact in the system while its trust level improves (i.e., increases) according to its interaction. The credit assignment process considers the node's dispositional trust level and the amount of credits reflects the nodes interaction in the system.

B. Social Trust Computation

After setup, ULOOP nodes activate their *trust table*. The trust table is a structure where each row is a tuple with the following structure: $\langle \text{Node Id}, \text{trust level}, \text{ageing} \rangle$. The table is periodically and passively built based on recommendations heard by the node, based on the computation of specific trust levels which represent costs of an association between two nodes, based on their users' willingness to share resources and based on their users' cooperating behavior (social behavior).

C. Cooperation and Rewarding

After a boot-up phase, executed only once, we proceed by activating two periodic activities of the *Cooperation Manager* and of the *Reward Manager*. The Cooperation Manager manages credits to motivate volunteer cooperation, and the Reward Manager manages credits when a gateway is only willing to cooperate if rewarded by its actions. After the phase where periodic activities are started, an ULOOP device enters the data transfer phase, which encompasses all the activities performed when data needs to be exchanged between nodes and gateways. Trust management itself starts each time a node attempts to perform regular MAC authentication, i.e., each time a ULOOP node is in the vicinity of some gateways. Due to regular scanning and overhearing, ULOOP nodes get ULOOP beacons (extension of regular Wi-Fi beacons) that allow them to understand if there are available gateways around. Before MAC authentication, it is necessary for a node to trust some gateways. Hence each node relies on the social trust level that it has toward neighbour gateways: if such value does not exist, the node will compute it based on a social trust computation

function. The computed trust level will be used by a requester (node) to select the most trustful potential requestee (gateway), with which the requester will initiate a cooperation session: the cooperation session may include the establishment of a reward. If the cooperation section is established with success (in case of volunteer cooperation or if credits allocated by requester are above the threshold established by a requestee that wants to be rewarded), the requester will start the resource management procedure. Otherwise the requester will look for another trustful gateway with whom it will try to establish a cooperation session.

D. Demo Description

The demo provides an overview of the trust management framework, starting with a regular Wi-Fi capable device attempting to associate to an ULOOP-enabled wireless network. The demo starts by showing how ULOOP software can be bootstrapped both to the User Equipment, based on an Android device, as well as how it can be bootstrapped to a OpenWRT Wi-Fi access point. Then the demo shows the process of trust setup that runs in the background, where the user shall only intervene one time. We then go over an example on trust negotiation, explaining what happens both from the perspective of the device requesting an association, and from the perspective of the device providing such association. The final part of the demo gives insight onto the rewarding framework which is most suitable when ULOOP is applied to an environment controlled by an entity that is willing to adopt a retailer cost model.

III. SUMMARY

Trust Management in ULOOP is used to obtain security in a flexible way without the use of strong security associations. The ULOOP trust management scheme includes a combination of the user's willingness to share network resources with others (dispositional trust), and a dynamic way to compute the cost of trust associations between devices owned by different users (social trust computation) based on devices interactions in terms of resources shared, as well as a mechanism to boost exchange in the face of untrusted environments (credits).

ACKNOWLEDGEMENTS

This work has been developed under the EU IST FP7 project ULOOP - User-centric Wireless Local Loop - grant number 247158.

REFERENCES

- [1] EU FP7 ULOOP Project, <http://www.uloop.eu>.
- [2] Rute Sofia (editor). D3: ULOOP High Level Architecture Specification. EU FP7 IST ULOOP project (grant number 257418) deliverable, December 2011.
- [3] Carlos Ballester, Jean-Marc Seigneur, Rute Sofia, Christian Silva, Waldir Moreira, and Alessandro Bogliolo. Trust Management in ULOOP. ULOOP White Paper 07. October 2012.