Anonymous Communication Using Wearables and Constrained Devices

Raúl Casanova Marqués  Jan Hajný
Brno University of Technology, Brno, CZ, {casanova, hajny}@feec.vutbr.cz

Abstract
Privacy problems in wearable and constrained devices can be solved using security mechanisms. However, problems related to location recognition do not have an immediate solution since an attacker may not have access to the information that is transmitted, but may discover which path it has traveled, who the source is, and even know who the destination is, threatening the anonymity of the users. A possible solution to address this problem is the communication of these devices by routing through anonymous networks.

1 Introduction
In recent years, developments related to the Internet of Things (IoT) have experienced a significant growth thanks to technological advances and miniaturization of hardware, producing an exponential increase in connected devices. According to a study published in Future Generation Computing Systems [1], around 24 billion devices are expected by 2020.

Within the IoT two different kind of devices can be found, wearables and constrained devices. On the one hand, wearable devices refer to the set of electronic devices that are incorporated somewhere in our body, such as intelligent clocks, sneakers with GPS or bracelets that control our health state. On the other hand, constrained devices which are small devices with limited CPU resources, memory and energy, often used as sensors or intelligent objects.

This kind of devices are being greatly accepted and implemented in society thanks to the benefits and facilities offered to users, for example, allowing them to make electronic payments, the possibility of assessing the vital signs, or notifying emergencies in case of irregular heart rhythm.

However, they are not exempt from problems that may affect the privacy and anonymity of users. Many of these devices already have security measures in place to protect privacy but do not have mechanisms to anonymize their location, allowing an attacker to obtain information about the location of the device.

There are anonymous networks such as Tor, I2P or FreeNet that are used to mask the identity of users and send data by a nondirect path to ensure anonymity in communications. Incorporating to these devices the possibility of accessing anonymous networks would solve the problems of anonymity and location tracking.

Fig. 1: Communication through anonymous networks
An example of anonymous routing using the Tor network on wearable and constrained devices is shown in Figure 1. These devices establish a connection through an intermediate node (Middle Relay, MR) of the network. The information is retransmitted anonymously through other MRs across the network until it finally reaches its destination through the exit node (Exit Relay, ER).

2 Security Challenges

Wearable and constrained devices are exposed to a series of threats that can endanger the privacy and anonymity of users. It is necessary that these devices have security measures to ensure anonymity in communications, as well as protecting confidential information by using encryption mechanisms.

Although many of these devices already have these mechanisms to preserve the privacy of users, they cannot guarantee their anonymity by allowing them to be located and thus obtain their location. The low computing capacity and limited resources of wearable and constrained devices make it very difficult to implement some security mechanisms and complicated algorithms in the devices that preserve anonymity without affecting other aspects such as battery life or device performance.

Some existing attacks against wearable and constrained devices have been studied ([2], [3]), as well as security threats in wireless communications. Attacks such as Wifi Hijacking, Man in the Middle, or Session Hijacking are common in these types of devices. It also explains some possible mitigations such as securing communications by validating the identity of users when trying to establish a new connection.

3 Existing Solutions in Anonymous Routing

Some anonymous routing schemes have been proposed such as Secure Distributed Anonymous Routing (SDAR [4]), ANonymous On Demand Routing (ANODR [5], MASK [6, 7]) with the aim of ensuring anonymity in communications. Furthermore, there are widely used anonymous networks, for example, Tor [8], I2P [9] and FreeNet [10].

SDAR [4]: All the nodes in an environment depend on a central node, which generates random keys depending on the level of trust they obtain. When a route discovery request is sent, it travels with a temporary key (TPK) and its secret key (TSK) encrypted with the public key of the destination. The nodes through which the packet passes use TPK to encrypt their own information by adding it to the packet. When it reaches the destination, it obtains the TSK and the information of all the nodes through which the packet has passed. The disadvantage of this system is that the destination knows all the intermediate nodes and their shared “secrets”, so the destination can know all the details of the source including its identity.

ANODR [5]: It is an on-demand routing protocol in which the origin launches a RREQ route request and the destination returns a RREP route response. Each node it passes through adds its secret and relays to it, and can share its secret with the successor and predecessor nodes. These secrets are used to encrypt and decrypt the message at each hop so the message changes appearance at each hop. The drawback is that each node in the path can see the original messages so if two or more nodes collude they can find out if they are on the same route and discover other nodes in that route.

MASK [6, 7]: In this system the neighbor authentication is done in the Medium Access Control (MAC) layer. Each pair of nodes shares a master key and generates a group of shared secrets with that master key. In the routing phase, it encrypts and decrypts messages using the secret shared between them. To reduce costs, an ARREQ routing request packet has the identity of the destination in plain text. The problem of this system is that each node or attacker that receives the ARREQ knows who the destination is. It therefore does not have anonymity of the destination.
node.

Tor [8], I2P [9] and FreeNet [10]: As privacy takes hold on the Internet, more and more users are choosing to use different services to avoid leaving traces on the network. Each of these networks has been developed for different uses and purposes, so not all have the same characteristics, however, all pursue the same goal, preserve the anonymity of their users. The main problem is the resources needed for these networks to work properly in wearable and constrained devices.

There is no global solution to preserve the anonymity of wearable devices. The first three solutions proposed (SDAR, ANODR, MASK) above may uncover data from the sender, receiver or path along which the information has circulated. However, Tor, I2P and FreeNet are more promising in the context of wearables and constrained devices because they implement mechanisms to protect the source and destination, as well as the communication path used.

4 Conclusion

The proposed anonymous routing protocols perform cryptographic operations on each hop during message transfer to make packets untraceable to external attackers, however, not all of them are resistant to internal attacks. In addition, due to high computational overhead they significantly degrade network performance.

Acknowledgements

The authors gratefully acknowledge funding from European Union’s Horizon 2020 Research and Innovation programme under the Marie Sklodowska Curie grant agreement No. 813278 (A-WEAR, http://www.a-wear.eu/)

References


